Lei 5,55

ION D. ION
A. GHIOCA
N. NEDIȚĂ

⊕	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

XII

Matematică

Algebră

Manual pentru clasa a XII-a

Editura didactică și pedagogică, București - 1981

A. P. GHIOCA
ION D. ION
N. I. NEDIȚĂ

Matematică

XII

Algebră

Manual pentru clasa a XII-a

Editura didactică și pedagogică
București

Manualul a fost elaborat în 1979 și revizuit în 1980 pe baza programei școlare aprobate de Ministerul Educației și Învățământului cu nr. 39490/1978.

Referenți: Prof. univ. **Gh. Galbură**
Prof. **Florina Saon**
Prof. **Maria Țuțuian**
Prof. **I. Țuțuian**
Prof. **I. V. Maftei**

Prezenta ediție a manualului de algebră pentru clasa a XII-a este rezultatul unei substanțiale revizii a celui apărut în anul 1979. S-a redus încărcătura teoretică a manualului, consecință și a restructurării problematicii programei școlare. A sporit numărul exemplelor și exercițiilor, introducîndu-se și modele de rezolvare pentru tipurile mai semnificative. Într-un capitol introductiv s-a realizat recapitularea unor teme despre mulțimi, funcții, matrice și numere, cu intenția de a instala pe cititor în lumea obiectelor matematice care sînt apoi sistematic invocate pentru ilustrarea teoriei structurilor algebrice.

Exercițiile cu asterisc de la sfîrșitul fiecărui capitol se adresează elevilor cu un interes sporit pentru matematică, rezolvarea lor nefiind necesară pentru parcurgerea manualului.

Autorii mulțumesc pe această cale referenților pentru sugestiile făcute, profesorilor de matematică din municipiul București, din județele Brașov, Brăila, Prahova și Vrancea care au inițiat și realizat un fructuos dialog asupra manualului.

Redactor: Prof. **Valentin Radu**
Tehnoredactor: **Constantina Velcovici**
Coperta: **N. Sîrbu**

Capitolul I — PRELIMINARII

§ 1. NUMERE

Peste tot în acest manual vom nota cu **N** mulțimea numerelor naturale,

$$\mathbf{N} = \{0, 1, 2, \ldots, n, \ldots\}.$$

Referitor la adunarea și înmulțirea numerelor naturale acceptăm proprietățile:

1) $(x + y) + z = x + (y + z)$,
2) $0 + x = x + 0 = x$,
3) $x + y = y + x$,
4) $(xy)z = x(yz)$,
5) $1 \cdot x = x \cdot 1 = x$,
6) $x(y + z) = xy + xz$,
7) $xy = yx$

oricare ar fi $x, y, z \in \mathbf{N}$.

De asemenea, vom nota cu **Z**, mulțimea numerelor întregi,

$$\mathbf{Z} = \{\ldots, -n, \ldots, -2, -1, 0, 1, 2, \ldots, n, \ldots\}.$$

Acceptăm ca adevărate pentru adunarea și înmulțirea numerelor întregi proprietățile 1) —7) precum și proprietatea:

8) $x + (-x) = (-x) + x = 0, \qquad \forall x \in \mathbf{Z}.$

Vom nota cu **Q** mulțimea numerelor raționale, $\mathbf{Q} = \{a/b \mid a, b \in \mathbf{Z}, b \neq 0\}$. Pentru $x \in \mathbf{Q}$, $x \neq 0$, $x = a/b$, notăm cu x^{-1} numărul rațional b/a. Avem:

9) $xx^{-1} = x^{-1}x = 1, \qquad \forall x \in \mathbf{Q},\ x \neq 0.$

Cu **R** va fi notată mulțimea numerelor reale iar cu **C** mulțimea numerelor complexe, $\mathbf{C} = \{a + ib \mid a, b \in \mathbf{R}\}$. Pentru adunarea și înmulțirea numerelor reale (complexe) acceptăm ca adevărate proprietăți 1) — 9).
Avem:

$$\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}.$$

Literele folosite mai sus pentru notarea mulțimilor de numere menționate apar în textul manualului culese gras (aldin). Pentru scrierea lor cu mîna (pe hîrtie sau la tablă...) la literele de tipar uzuale se adaugă o linie suplimentară. Aceste convenții de notații sînt consacrate în literatura matematică actuală.

§ 2. MULȚIMI ȘI FUNCȚII (recapitulare)

Fie E o mulțime. Vom nota cu $\mathcal{P}(E)$ mulțimea tuturor părților (submulțimilor) lui E. Dacă $X, Y \in \mathcal{P}(E)$, atunci cu $X \cup Y$ și $X \cap Y$ vom nota *reuniunea*, respectiv *intersecția* lui X cu Y,

$$X \cup Y \stackrel{\text{def}}{=} \{x \in E \mid x \in X \text{ sau } x \in Y\}$$

respectiv

$$X \cap Y \stackrel{\text{def}}{=} \{x \in E \mid x \in X \text{ și } x \in Y\}.$$

Amintim următoarele proprietăți ale reuniunii și intersecției:

1) $(X \cup Y) \cup Z = X \cup (Y \cup Z)$, $(X \cap Y) \cap Z = X \cap (Y \cap Z)$;

2) $\varnothing \cup X = X \cup \varnothing = X$, $E \cap X = X \cap E = X$;

3) $X \cup Y = Y \cup X$, $X \cap Y = Y \cap X$;

4) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$, $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$

oricare ar fi $X, Y, Z \in \mathcal{P}(E)$, unde $\varnothing$ este submulțimea *vidă* a lui E.

Fie E și F două mulțimi. Pentru o funcție $f : E \to F$ vom preciza uneori și acțiunea lui f asupra elementelor $x \in E$ prin notația

$$f : E \to F, \quad x \to f(x)$$

unde $f(x)$ este *imaginea* lui x prin f.

Fie E o mulțime. Vom nota cu $\mathcal{F}(E)$ mulțimea tuturor funcțiilor $f : E \to E$. Dacă $f, g \in \mathcal{F}(E)$, atunci funcția

$$h : E \to E, \quad x \to h(x) \stackrel{\text{def}}{=} f(g(x))$$

se notează cu $f \circ g$ și se numește *compusa* funcției f cu funcția g (v. fig. I.1)

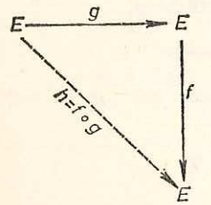


Fig. I.1.

Funcția $1_E : E \to E$, $1_E(x) = x$, $\forall x \in E$, se numește *aplicația identică* a mulțimii E.

2.1. **Teoremă. Compunerea funcțiilor are proprietățile:**

1) $(f \circ g) \circ h = f \circ (g \circ h)$ $\quad \forall f, g, h \in \mathcal{F}(E)$,

2) $1_E \circ f = f \circ 1_E = f$ $\quad \forall f \in \mathcal{F}(E)$.

Demonstrație. Pentru orice $x \in E$ avem:

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$$

și

$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$$

de unde

$$(f \circ g) \circ h = f \circ (g \circ h).$$

De asemenea, pentru orice $x \in E$ avem:

$$(1_E \circ f)(x) = 1_E(f(x)) = f(x) = f(1_E(x)) = (f \circ 1_E)(x),$$

deci

$$1_E \circ f = f \circ 1_E = f.$$

O funcție $f : E \to F$ se numește *injectivă* dacă $f(x_1) \neq f(x_2)$ oricare ar fi $x_1, x_2 \in E$, $x_1 \neq x_2$, ceea ce revine la:

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

Spunem că funcția $f : E \to F$ este *surjectivă* dacă:

$$\forall y \in F, \exists x \in E \text{ astfel încît } y = f(x).$$

O funcție $f : E \to F$ se numește *bijectivă* dacă este injectivă și surjectivă.

2.2. **Teoremă. Fie E o mulțime și $f, g \in \mathcal{F}(E)$. Dacă f și g sînt funcții injective (surjective, bijective) atunci $f \circ g$ este funcție injectivă (respectiv surjectivă, bijectivă).**

Demonstrație. Fie $h = f \circ g$. Presupunem că f și g sînt injective și fie $x_1, x_2 \in E$ astfel încît $h(x_1) = h(x_2)$. Rezultă că $f(g(x_1)) = f(g(x_2))$. Cum f este funcție injectivă rezultă că $g(x_1) = g(x_2)$, de unde $x_1 = x_2$ căci și g este funcție injectivă. Așadar $h = f \circ g$ este funcție injectivă.

Presupunem că f și g sînt funcții surjective și fie $z \in E$. Cum f și g sînt funcții surjective, există $y \in E$ astfel încît $z = f(y)$ și există $x \in E$ astfel încît $y = g(x)$, de unde

$$z = f(y) = f(g(x)) = (f \circ g)(x) = h(x),$$

deci $h = f \circ g$ este funcție surjectivă. Ultima afirmație este acum evidentă.

Dacă E și F sînt două mulțimi, vom nota cu $E \setminus F$ mulțimea

$$E \setminus F = \{x \in E \mid x \notin F\}$$

numită *diferența* dintre E și F (în această ordine). Cu $E \times F$ vom nota *produsul cartezian* al lui E cu F, adică mulțimea tuturor perechilor ordonate (x, y), cu $x \in E$ și $y \in F$,

$$E \times F \stackrel{\text{def}}{=} \{(x, y) \mid x \in E, y \in F\}.$$

§ 3. MATRICE (recapitulare)

Notăm cu $M_2(\mathbb{R})$ mulțimea tuturor matricelor pătratice A de ordin 2 cu coeficienți din $\mathbb{R}$,

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad a_{ij} \in \mathbb{R}.$$

Vom folosi și scrierea mai condensată: $A = (a_{ij})$.

Dacă $A, B \in M_2(\mathbb{R})$, $A = (a_{ij})$, $B = (b_{ij})$, atunci *suma* $A + B$ a matricei A cu matricea B se definește prin:

$$A + B \stackrel{\text{def}}{=} \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix} \in M_2(\mathbb{R}).$$

De asemenea, *produsul* AB al matricei A cu matricea B se definește prin:

$$AB \overset{\text{def}}{=} \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix} \in M_2(\mathbf{R}).$$

Matricele 0, E și $-A$ din $M_2(\mathbf{R})$,

$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad -A = \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}$$

se numesc respectiv *matricea zero*, *matricea unitate*, *opusa matricei* A.

Avem următoarele proprietăți ale adunării și înmulțirii matricelor din $M_2(\mathbf{R})$:

1) $(A + B) + C = A + (B + C)$,
2) $0 + A = A + 0 = A$,
3) $A + (-A) = (-A) + A = 0$,
4) $A + B = B + A$,
5) $(AB)C = A(BC)$,
6) $EA = AE = A$,
7) $A(B + C) = AB + AC$; $\quad (B + C)A = BA + CA$

oricare ar fi A, B, $C \in M_2(\mathbf{R})$. După cum se știe din clasa a XI-a, demonstrarea lor se face invocînd proprietăți similare ale operațiilor cu numere reale. Astfel:

$$A + (-A) = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + (-a_{11}) & a_{12} + (-a_{12}) \\ a_{21} + (-a_{21}) & a_{22} + (-a_{22}) \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$$

și analog, $(-A) + A = 0$.

Vom nota cu $M_2(\mathbf{Z})$, $M_2(\mathbf{Q})$, $M_2(\mathbf{C})$ mulțimea matricelor pătratice de ordin 2 cu coeficienți în $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{C}$ respectiv. În general, pentru $n > 1$, notăm cu $M_n(\mathbf{Z})$, $M_n(\mathbf{Q})$, ... mulțimea matricelor pătratice de ordin n cu coeficienți în $\mathbf{Z}$, $\mathbf{Q}$, ... respectiv.

Dacă $A \in M_2(\mathbf{R})$, $A = (a_{ij})$, vom nota cu $\det(A)$ *determinantul* matricei A,

$$\det(A) = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{21}a_{12} \in \mathbf{R}.$$

3.1. **Teoremă. Oricare ar fi** A, $B \in M_2(\mathbf{R})$, $A = (a_{ij})$, $B = (b_{ij})$, **avem:**

$$\det(AB) = \det(A) \det(B).$$

Demonstrație. Avem:

$$AB = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}.$$

Pe de altă parte, se observă că avem identitatea:

$$(a_{11}b_{11} + a_{12}b_{21})(a_{21}b_{12} + a_{22}b_{22}) - (a_{21}b_{11} + a_{22}b_{21})(a_{11}b_{12} + a_{12}b_{22}) =$$
$$= (a_{11}a_{22} - a_{21}a_{12})(b_{11}b_{22} - b_{21}b_{12}),$$

de unde

$$\det(AB) = \det(A) \det(B).$$

Exemplu.

Dacă $A \in M_2(\mathbf{R})$, $A = \begin{pmatrix} 2 & 1 \\ 5 & 2 \end{pmatrix}$, atunci

$$\det(A^n) = (-1)^n \text{ oricare ar fi } n = 1, 2, \ldots .$$

În adevăr, $\det(A) = 2 \times 2 - 5 \times 1 = -1$ și deci afirmația este adevărată pentru $n = 1$. Presupunem că $n > 1$ și că $\det(A^{n-1}) = (-1)^{n-1}$. Atunci:

$$\det(A^n) = \det(A^{n-1} \cdot A) = \det(A^{n-1}) \det(A) = (-1)^{n-1} \cdot (-1) = (-1)^n.$$

§ 4. NUMERE RELATIV PRIME (recapitulare)

Fie a și b două numere întregi. Un număr $d \in \mathbf{Z}$, $d \geqslant 0$, se numește *cel mai mare divizor comun* (c.m.m.d.c.) al lui a și b dacă:

(1) $d \mid a$ și $d \mid b$;
(2) $c \mid a$ și $c \mid d \Rightarrow c \mid d$.

Dacă $d' \in \mathbf{Z}$, $d' \geqslant 0$, satisface, de asemenea, (1) și (2), atunci avem $d' \mid d$ și $d \mid d'$ de unde $d' = d$. Așadar, c.m.m.d.c. al numerelor a și b, în caz că există, este unic determinat. Pentru c.m.m.d.c. al lui a și b folosim notația $d = (a, b)$.

4.1. **Teoremă. Fie** a, $b \in \mathbf{Z}$. **Atunci c.m.m.d.c. al lui** a **și** b **există. Mai mult, dacă** $d = (a, b)$, **atunci există** h, $k \in \mathbf{Z}$ **astfel încît**

$$d = ah + bk.$$

Demonstrație. Dacă $a = b = 0$, atunci $d = 0$, și $0 = 0h + 0k$, unde h, k pot fi luați chiar arbitrar din $\mathbf{Z}$ în acest caz.

Presupunem că $a \neq 0$ sau $b \neq 0$. Fie $d = ah + bk$ cel mai mic număr strict pozitiv printre numerele de forma:

$$ax + by \qquad x, y \in \mathbf{Z}$$

(arătați că printre ele se găsesc numere strict pozitive!).

Dacă $c \mid a$ și $c \mid b$, atunci c divide și pe $ah + bk = d$, deci d satisface (2) din definiția c.m.m.d.c. Rămîne să mai arătăm că $d \mid a$ și $d \mid b$.

Dacă d nu divide pe a, există q, $r \in \mathbf{Z}$ astfel încît

$$a = dq + r, \qquad 0 < r < d.$$

. Atunci

$0 < r = a - dq = a - (ah + bk)q = a(1 - hq) + b(-kq) < d$, ceea ce contrazice alegerea lui d. Rămîne adevărat că $d \mid a$. Analog se arată că $d \mid b$.

Fie $a, b \in \mathbf{Z}$. Vom spune că a este *relativ prim* cu b dacă $(a, b) = 1$. Evident, a este relativ prim cu b dacă și numai dacă există $h, k \in \mathbf{Z}$ astfel încît $ah + bk = 1$.

4.2. **Teoremă. Fie $a, b, c, \in \mathbf{Z}$. Avem:**

1) **Dacă** $(a, b) = 1$ **și** $(a, c) = 1 \Rightarrow (a, bc) = 1$;

2) **Dacă** $(a, b) = 1$ **și** $a \mid bc \Rightarrow a \mid c$;

3) **Dacă** $(a, b) = 1$, $a \mid c$ **și** $b \mid c \Rightarrow ab \mid c$.

Demonstrație. 1) Fie $h, k, u, v \in \mathbf{Z}$ astfel încît $1 = ah + bk$ și $1 = au + cv$. Atunci:

$1 = ah + bk(au + cv) = a(h + bku) + bc(kv)$, de unde $(a, bc) = 1$.

2) Fie $h, k \in \mathbf{Z}$ astfel încît $ah + bk = 1$. Atunci $c = a(hc) + bck$. Cum $a \mid a$ și $a \mid bc$ rezultă că a divide numărul $a(hc) + bc \cdot k = c$.

3) Fie $h, k \in \mathbf{Z}$ astfel încît $ah + bk = 1$. Atunci $c = ac \cdot h + bc \cdot k$. Cum $a \mid c$ și $b \mid c$ rezultă că $ab \mid ac$ și $ab \mid bc$, deci ab divide numărul $ac \cdot h + bc \cdot k = c$.

Exemple

1. Dacă $p > 0$ este un număr prim, atunci:

$$(a, p) = 1 \qquad \forall a \in \mathbf{Z}, \qquad 1 \leqslant a < p.$$

În adevăr, p fiind număr prim, singurii săi divizori pozitivi sînt 1 și p. Cum $1 \leqslant a < p$, p nu poate divide pe a. Rezultă că singurul divizor comun al lui a și p este 1 și atunci și c.m.m.d.c. al lui a și p este 1.

2. Pentru orice $n \in \mathbf{N}$, numărul $n^3 - n$ se divide prin 6. În adevăr, $n^3 - n = (n - 1)n(n + 1)$, deci $n^3 - n$ se divide prin 2 și 3. Cum $(2, 3) = 1$, rezultă că $n^3 - n$ se divide și prin $2 \times 3 = 6$.

3. Dacă $p > 0$, $q > 0$ sînt două numere prime distincte, atunci:

$$(p^m, q^n) = 1 \qquad \forall m, n \in \mathbf{N}.$$

În adevăr, să presupunem că $p < q$. Atunci conform cu rezultatul de la Exp. 1 avem $(p, q) = 1$. Presupunem că $(p, q^{n-1}) = 1$. Folosind Teorema 4.2, pct. 1) din $(p, q) = 1$ și $(p, q^{n-1}) = 1$ rezultă $(p, q^n) = 1$. Acum se fixează n și se demonstrează prin inducție asupra lui m că $(p^m, q^n) = 1$.

§ 5. NUMERE PĂTRATICE

Se știe că $\sqrt{2}$ nu este număr rațional. Să reamintim demonstrația. Dacă $\sqrt{2} \in \mathbf{Q}$, atunci $\sqrt{2} = a/b$, cu $a, b \in \mathbf{Z}$, $b \neq 0$. Putem presupune că fracția a/b este ireductibilă, adică a și b nu admit nici un divizor comun $c \in \mathbf{Z}$ astfel

încît $|c| > 1$. Cum $a^2 = 2b^2$ rezultă că a^2 este par, deci a este par, de unde $a = 2a_1$, cu $a_1 \in \mathbf{Z}$. Avem $4a_1^2 = 2b^2$, deci $2a_1^2 = b^2$. Rezultă că și b este par, deci a și b admit ca divizor comun pe 2. Contradicție.

5.1. *Definiție.* **Spunem că un număr întreg d diferit de 0 și 1 este *liber de pătrate* dacă nu se divide prin pătratul nici unui număr prim.**

Astfel numerele 6, 2, -15, -1, -3 sînt libere de pătrate. Numerele 108 și -40 nu sînt libere de pătrate căci $108 = 3^3 \cdot 2^2$, $-40 = (-5) \cdot 2^3$.

Dacă $d \geqslant 0$ atunci prin $\sqrt{d}$ notăm radicalul aritmetic al lui d adică unicul număr real $\alpha \geqslant 0$ astfel încît $\alpha^2 = d$. Dacă $d < 0$, atunci $\sqrt{d} = i\sqrt{-d}$, unde $i^2 = -1$. Astfel $\sqrt{-3} = i\sqrt{3}$.

5.2. **Teoremă. Dacă d este un număr întreg liber de pătrate, atunci $\sqrt{d} \notin \mathbf{Q}$.**

Demonstrație. Dacă $d < 0$, atunci $\sqrt{d}$ este număr complex și deci $\sqrt{d} \notin \mathbf{Q}$. Rămîne să considerăm cazul $d > 1$. Dacă $\sqrt{d} \in \mathbf{Q}$ atunci $d = a/b$, $a > 0$, $b > 0$ unde a/b este o fracție ireductibilă. Avem $db^2 = a^2$ și dacă $a = 1$, atunci $b^2 d = 1$, deci $d = 1$. Contradicție. Deci $a > 1$ și atunci a admite un divizor prim p. Așadar $a = pc$, cu $c \in \mathbf{Z}$, de unde $b^2 d = p^2 c^2$. Cum fracția a/b este ireductibilă, p nu divide pe b, deci din egalitatea $b^2 d = p^2 c$ rezultă că p^2 divide pe d. Contradicție.

Numerele de forma $a + b\sqrt{d}$, cu $a, b \in \mathbf{Q}$ și d întreg liber de pătrate se numesc *numere pătratice*. Astfel:

$$1 + \sqrt{2}, \quad \frac{-1 + \sqrt{-3}}{2} = \frac{-1 + i\sqrt{3}}{2}, \quad 4 + 3\sqrt{5}, \quad 2 - 3i$$

sînt numere pătratice, unde $i^2 = -1$.

Dacă $a + b\sqrt{d}$ și $a' + b'\sqrt{d}$ sînt două numere pătratice, atunci:

$$a + b\sqrt{d} = a' + b'\sqrt{d} \Leftrightarrow a = a' \text{ și } b = b'.$$

În adevăr, dacă $a + b\sqrt{d} = a' + b'\sqrt{d}$ și $b \neq b'$, atunci

$$\sqrt{d} = \frac{a - a'}{b - b'} \in \mathbf{Q}$$

Contradicție. Deci $b = b'$ și atunci $a = a'$.

Dacă d este un întreg liber de pătrate, atunci notăm cu $\mathbf{Q}(\sqrt{d})$ mulțimea tuturor numerelor pătratice de forma $a + b\sqrt{d}$, cu $a, b \in \mathbf{Q}$ și cu $\mathbf{Z}[\sqrt{d}]$ mulțimea tuturor numerelor pătratice de forma $a + b\sqrt{d}$ cu $a, b \in \mathbf{Z}$. Așadar:

$$\mathbf{Q}(\sqrt{d}) \overset{\text{def}}{=} \{a + b\sqrt{d} \mid a, b \in \mathbf{Q}\}$$

și

$$\mathbf{Z}[\sqrt{d}] \overset{\text{def}}{=} \{a + b\sqrt{d} \mid a, b \in \mathbf{Z}\}.$$

Evident

$$\mathbb{Z} \subset \mathbb{Z}[\sqrt{d}] \subset \mathbb{Q}(\sqrt{d}) \subset \mathbb{C},$$

iar cînd $d > 0$, avem chiar $\mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$.
Astfel:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subset \mathbb{R}$$

și

$$Z[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

Dacă $z = a + b\sqrt{d}$ este un număr pătratic, atunci numărul pătratic $z^* = a - b\sqrt{d}$ se numește *conjugatul* lui z iar numărul rațional nenegativ

$$N(z) \overset{\text{def}}{=} |zz^*| = |a^2 - db^2| \geqslant 0$$

se numește *norma* lui z.

Astfel, dacă $z = 3 + \sqrt{2}$, atunci $z^* = 3 - \sqrt{2}$ și $N(z) = |zz^*| = |3^2 - 2 \cdot 1^2| = |7| = 7$.

Dacă $z = \frac{-1}{2} + \frac{\sqrt{-3}}{2}$, atunci $z^* = -\frac{1}{2} - \frac{\sqrt{-3}}{2}$ și $N(z) = |zz^*| = \left|\left(-\frac{1}{2}\right)^2 + 3\left(\frac{1}{2}\right)^2\right| = 1$.

5.3. **Teoremă. Fie d un întreg liber de pătrate și $z_1, z_2 \in \mathbb{Q}(\sqrt{d})$, $z_1 = a_1 + b_1\sqrt{d}$, $z_2 = a_2 + b_2\sqrt{d}$.**
Atunci:

1) $z_1 + z_2 \in \mathbb{Q}(\sqrt{d})$, $z_1 z_2 \in \mathbb{Q}(\sqrt{d})$;
2) $(z_1 + z_2)^* = z_1^* + z_2^*$, $(z_1 z_2)^* = z_1^* z_2^*$, $(z_1^*)^* = z_1$;
3) $N(z_1 z_2) = N(z_1)N(z_2)$.

Demonstrație. 1) Cum a_1, a_2, b_1 și b_2 sînt numere raționale și

$$z_1 + z_2 = (a_1 + b_1\sqrt{d}) + (a_2 + b_2\sqrt{d}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{d},$$
$$z_1 z_2 = (a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = (a_1 a_2 + db_1 b_2) + (a_1 b_2 + a_2 b_1)\sqrt{d},$$

rezultă că $z_1 + z_2 \in \mathbb{Q}(\sqrt{d})$ și $z_1 z_2 \in \mathbb{Q}(\sqrt{d})$.

2) Avem:

$$(z_1 + z_2)^* = (a_1 + a_2) - (b_1 + b_2)\sqrt{d} = (a_1 - b_1\sqrt{d}) + (a_2 - b_2\sqrt{d}) =$$
$$= z_1^* + z_2^*, \quad (z_1 z_2)^* = (a_1 a_2 + db_1 b_2) - (a_1 b_2 + a_2 b_1)(\sqrt{d}) =$$
$$= (a_1 - b_1\sqrt{d})(a_2 - b_2\sqrt{d}) = z_1^* z_2^*, \quad (z_1^*)^* = (a_1 - b_1\sqrt{d})^* =$$
$$= a_1 - (-b_1)\sqrt{d} = a_1 + b_1\sqrt{d} = z_1.$$

3) Avem:

$$N(z_1 z_2) = |z_1 z_2 (z_1 z_2)^*| = |z_1 z_2 z_1^* z_2^*| = |(z_1 z_1^*)(z_2 z_2^*)| = |z_1 z_1^*| \cdot |z_2 z_2^*| =$$
$$= N(z_1)N(z_2).$$

Exerciții rezolvate

R—1 Fie E o mulțime și $f, g \in \mathfrak{F}(E)$. Avem:

1) Dacă $f \circ g$ este funcție injectivă (surjectivă) atunci g este funcție injectivă (resp. f este funcție surjectivă);

2) Dacă $f \circ g = 1_E$, atunci g este funcție injectivă și f este funcție surjectivă;

3) Dacă $f \circ g = g \circ f = 1_E$, atunci f și g sînt funcții bijective.

Soluție. 1) Presupunem că $f \circ g$ este funcție injectivă și fie $x_1, x_2 \in E$ astfel încît $g(x_1) = g(x_2)$. Atunci

$$(f \circ g)(x_1) = f(g(x_1)) = f(g(x_2)) = (f \circ g)(x_2).$$

Cum $f \circ g$ este funcție injectivă, deducem $x_1 = x_2$, deci g este funcție injectivă.
Fie $z \in E$. Dacă $f \circ g$ este funcție surjectivă, atunci există $x \in E$ astfel încît

$$z = (f \circ g)(x) = f(g(x)).$$

Rezultă că $z = f(y)$, unde $y = g(x) \in E$, deci f este funcție surjectivă.
2) Rezultă din 1) observînd că 1_E este funcție injectivă și surjectivă.
3) Rezultă din 2).

R—2 Fie $E = \mathbf{Z} \times \mathbf{Z}$ și $A = \begin{pmatrix} 2 & 3 \\ -1 & -2 \end{pmatrix}$. Definim funcția:

$$f_A : E \to E, \quad f_A(x) = (2x_1 + 3x_2, \ -x_1 - 2x_2) \quad \forall x = (x_1, x_2) \in E.$$

Arătați că:

1) $f_A \circ f_A = 1_E$,
2) f_A este funcție bijectivă.

Soluție. 1) Pentru orice $x \in E$, $x = (x_1, x_2)$ avem

$$(f_A \circ f_A)(x) = f_A(f_A(x)) = f_A((2x_1 + 3x_2, -x_1 - 2x_2)) =$$
$$= (2(2x_1 + 3x_2) + 3(-x_1 - 2x_2), -x_1(2x_1 + 3x_2) - 2(-x_1 - 2x_2)) = (x_1, x_2) = x$$

de unde $f_A \circ f_A = 1_E$.
2) Rezultă din Ex. R-1, pct. 2).

R—3 Fie $U, A \in M_2(\mathbf{Z})$,

$$U = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}, \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

1) Găsiți o matrice $X \in M_2(\mathbf{Z})$ astfel încît $UX = E$;

2) Arătați că ecuația $AX = E$ admite o soluție $X \in M_2(\mathbf{Z})$ dacă și numai dacă $\det(A) = \pm 1$ și în acest caz avem și $XA = E$.

Soluție. 1) Fie $X = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$. Cum

$$UX = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 3x + z & 3y + w \\ 5x + 2z & 5y + 2w \end{pmatrix}$$

avem $UX = E$ dacă și numai dacă

$$\begin{pmatrix} 3x+2 & 3y+w \\ 5x+2z & 5y+2w \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

ceea ce revine la:

a) $\begin{cases} 3x + z = 1 \\ 5x + 2z = 0 \end{cases}$ și b) $\begin{cases} 3y + w = 0 \\ 5y + 2w = 1. \end{cases}$

Rezolvînd sistemele de mai sus găsim $x = 2$, $y = -5$, $y = -1$ și $w = 3$, deci

$$X = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} \in M_2(\mathbf{Z}).$$

2) Fie $X \in M_2(\mathbf{Z})$ astfel încît $AX = E$.

Atunci

$$1 = \det(E) = \det(AX) = \det(A)\det(X)$$

și cum $\det(A)$ și $\det(X)$ sînt numere întregi, rezultă că $\det(A) = \pm 1$.

Reciproc, dacă $\det(A) = \pm 1$, atunci urmînd calea de rezolvare de la pct. 1) se găsește:

$$X = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in M_2(\mathbf{Z}) \quad \text{dacă} \quad ad - cb = 1$$

și

$$X = \begin{pmatrix} -d & b \\ c & -a \end{pmatrix} \in M_2(\mathbf{Z}) \quad \text{dacă} \quad ad - cb = -1.$$

În ambele cazuri avem și $XA = E$.

R—4 Fie m_1 și m_2 doi întregi pozitivi relativ primi, $m = m_1 m_2$ și $\mathcal{R}_m = \{0, 1, 2, \ldots, m-1\}$, $\mathcal{R}_{m_1} = \{0, 1, \ldots, m_1 - 1\}$, $\mathcal{R}_{m_2} = \{0, 1, \ldots, m_2 - 1\}$.

Dacă $a, n \in \mathbf{Z}$, $n > 0$, atunci notăm cu $a \bmod n$ restul împărțirii lui a prin n.

1) Arătați că funcția

$$f : \mathcal{R}_m \to \mathcal{R}_{m_1} \times \mathcal{R}_{m_2},\ f(a) = (a \bmod m_1,\ a \bmod m_2)\ \forall a \in \mathcal{R}_m$$

este bijectivă.

2) Enumerați valorile funcției f cînd $m_1 = 4$ și $m_2 = 3$.

Soluție. 1) Mulțimea $\mathcal{R}_m$ are m elemente și mulțimea $\mathcal{R}_{m_1} \times \mathcal{R}_{m_2}$ are $m_1 m_2 = m$ elemente.

Este deci suficient să arătăm că funcția f este injectivă. Fie $a, b \in \mathcal{R}_m$ astfel încît $f(a) = f(b)$. Atunci

$$(a \bmod m_1,\ a \bmod m_2) = (b \bmod m_1,\ b \bmod m_2).$$

Rezultă că $a \bmod m_1 = b \bmod m_1$ și $a \bmod m_2 = b \bmod m_2$. Cum $a \bmod m_1 = b \bmod m_1$, deducem că a și b dau același rest prin împărțirea cu m_1, deci $m_1 \mid (a - b)$. Analog se deduce că $m_2 \mid (a - b)$. Dar $(m_1, m_2) = 1$, deci $m_1 m_2 \mid (a - b)$. Cum $|a - b| < m$, rezultă $a - b = 0$, deci $a = b$. Așadar, f este funcție injectivă.

2) În acest caz $m = 4 \times 3 = 12$, $\mathcal{R}_{12} = \{0, 1, 2, \ldots, 11\}$, $\mathcal{R}_4 = \{0, 1, 2, 3\}$ și $\mathcal{R}_3 = \{0, 1, 2\}$. Avem:

$f(0) = (0, 0)$; $f(4) = (0, 1)$; $f(8) = (0, 2)$;
$f(1) = (1, 1)$; $f(5) = (1, 2)$; $f(9) = (1, 0)$;
$f(2) = (2, 2)$; $f(6) = (2, 0)$; $f(10) = (2, 1)$;
$f(3) = (3, 0)$; $f(7) = (3, 1)$; $f(11) = (3, 2)$.

Astfel:

$$f(7) = (7 \bmod 4,\ 7 \bmod 3) = (3, 1).$$

R—5 Fie $u \in \mathbf{Z}[\sqrt{2}]$, $u = 1 + \sqrt{2}$.

1) Arătați că $N(u^n) = 1$, $\forall n \geqslant 1$;

2) Determinați un număr $z \in \mathbf{Z}[\sqrt{2}]$ astfel încît $uz = 1$;

3) Fie $v \in \mathbf{Z}[\sqrt{2}]$, $v = a + b\sqrt{2}$ cu $a, b \in \mathbf{Z}$. Arătați că există $z \in \mathbf{Z}[\sqrt{2}]$ astfel încît $vz = 1$ dacă și numai dacă $N(v) = 1$;

4) Fie $v \in \mathbf{Q}(\sqrt{2})$, $v = a + b\sqrt{2}$ cu $a, b \in \mathbf{Q}$. Dacă $v \neq 0$ arătați că există $z \in \mathbf{Q}(\sqrt{2})$ astfel încît $vz = 1$.

Soluție. 1) Avem $N(u) = |uu^*| = |(1+\sqrt{2})(1-\sqrt{2})| = |-1| = 1$. Dacă $n > 1$ și $N(u^{n-1}) = 1$, atunci

$$N(u^n) = N(u^{n-1} \cdot u) = N(u^{n-1})N(u) = 1 \cdot 1 = 1,$$

deci 1) este demonstrat astfel prin inducție.

2) Observăm că $uu^* = -1$, deci $u(-u^*) = 1$, de unde $uz = 1$ cu $z = -u^* = -1 + \sqrt{2} \in \mathbf{Z}[\sqrt{2}]$. O altă cale de determinare a lui z este dată mai jos.

3) Dacă $z \in \mathbf{Z}[\sqrt{2}]$, $z = x + y\sqrt{2}$ cu $x, y \in \mathbf{Z}$, este astfel încît $vz = 1$, atunci

$$1 = N(1) = N(vz) = N(v)N(z) = |a^2 - 2b^2| \cdot |x^2 - 2y^2|.$$

Cum $N(v) \in \mathbf{N}$ și $N(z) \in \mathbf{N}$, deducem că $N(v) = 1$.

Reciproc, presupunem că $N(v) = 1$ și să determinăm $z \in \mathbf{Z}[\sqrt{2}]$, $z = x + y\sqrt{2}$ cu $x, y \in \mathbf{Z}$, astfel încît $vz = 1$.

Cum

$$1 + 0\sqrt{2} = 1 = vz = (a + b\sqrt{2})(x + y\sqrt{2}) = (ax + 2by) + (ay + bx)\sqrt{2},$$

rezultă că egalitatea $1 = vz$ este echivalentă cu sistemul de ecuații liniare

$$(*) \qquad \begin{cases} ax + 2by = 1, \\ bx + ay = 0. \end{cases}$$

Rezolvînd sistemul găsim:

$$z = a - b\sqrt{2} \qquad \text{cînd } a^2 - 2b^2 = 1$$

și

$$z = -a + b\sqrt{2} \qquad \text{cînd } a^2 - 2b^2 = -1.$$

4) Cum $v = a + b\sqrt{2} \neq 0$, rezultă $a \neq 0$ sau $b \neq 0$. Deducem că $a^2 - 2b^2 \neq 0$ (căci $a^2 - 2b^2 = 0$ și $\sqrt{2} \notin \mathbf{Q}$ atrage $b = 0$, deci și $a = 0$, adică $v = 0$).

Procedînd ca la pct. 3) se observă că pentru $z \in \mathbf{Q}(\sqrt{2})$, $z = x + y\sqrt{2}$ cu $x, y \in \mathbf{Q}$, egalitatea $vz = 1$ este echivalentă cu sistemul liniar

$$(**) \qquad \begin{cases} ax + 2by = 1, \\ bx + ay = 0. \end{cases}$$

Dar determinantul matricei sistemului (**) este egal cu $a^2 - 2b^2 \neq 0$. Rezultă că sistemul (**) are soluție (chiar unică), anume:

$$x = \frac{a}{a^2 - 2b^2} \in \mathbf{Q}, \qquad y = \frac{-b}{a^2 - 2b^2} \in \mathbf{Q}.$$

Așadar, avem $vz = 1$, unde

$$z = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbf{Q}(\sqrt{2}).$$

Exerciții

1. Fie $f : \mathbf{Z} \to \mathbf{Z}$, $f(x) = 2x + 1$, $\forall x \in \mathbf{Z}$. Arătați că:

1) f este funcție injectivă;

2) f nu este funcție surjectivă.

2. Fie $f : \mathbf{N} \to \mathbf{N}$, $f(x) = x + 1$, $\forall x \in \mathbf{N}$ și $g : \mathbf{N} \to \mathbf{N}$, $g(x) = x - 1$, $\forall x \in \mathbf{N}$, $x \neq 0$ și $g(0) = 0$. Arătați că:

1) f este injectivă și nu este surjectivă;

2) g este surjectivă și nu este injectivă;

3) $g \circ f = 1_N$.

3. Pentru $a, b \in \mathbf{R}$, $a \neq 0$, definim funcția $f_{a,b} : \mathbf{R} \to \mathbf{R}$, $f_{a,b}(x) = ax + b$, $\forall x \in \mathbf{R}$. Arătați că:

1) $f_{a,b}$ este funcție bijectivă;

2) $f_{a,b} \circ f_{c,d} = f_{ac,\, ad+b}$ $\forall a, b, c, d \in \mathbf{R}$, $a \neq 0$, $c \neq 0$.

3) Pentru $a, b \in \mathbf{R}$, $a \neq 0$, găsiți $\alpha, \beta \in \mathbf{R}$ astfel încît $f_{a,b} \circ f_{\alpha,\beta} = 1_{\mathbf{R}}$.

4. Fie $A \in M_2(\mathbf{Z})$, $A = \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix}$, $E = \mathbf{Z} \times \mathbf{Z}$, $F = \mathbf{Q} \times \mathbf{Q}$,

$$f_A : E \to E,\ f_A(x) = (3x_1 + x_2,\ 4x_1 + 2x_2)\ \forall x = (x_1, x_2) \in E,$$
$$f_A^* : F \to F,\ f_A^*(x) = (3x_1 + x_2,\ 4x_1 + 2x_2)\ \forall x = (x_1, x_2) \in F.$$

Arătați că:

1) f_A este funcție injectivă și nu este surjectivă.

2) f_A^* este bijectivă.

5. Fie $A \in M_2(\mathbf{Q})$, $A = \begin{pmatrix} -1/2 & 3/2 \\ -1/2 & -1/2 \end{pmatrix}$. Arătați că:

$$A^2 + A + E = 0,\ A^3 = E.$$

6. Pentru orice $\theta \in \mathbf{R}$ definim matricele:

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix},\quad S_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

Arătați că:

1) $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} R_{-\theta} = S_{-\theta}$, $R_\theta \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = S_\theta$, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = S_0$.

2) $R_\theta R_{\theta'} = R_{\theta+\theta'}$, $R_\theta S_{\theta'} = S_{\theta+\theta'}$, $S_\theta R_{\theta'} = S_{\theta-\theta'}$, $S_\theta S_{\theta'} = R_{\theta-\theta'}$.

3) $R_\theta R_{-\theta} = R_{-\theta} R_\theta = E$, $S_\theta S_\theta = E$.

7. Pentru o matrice $A \in M_2(\mathbf{R})$ următoarele afirmații sînt echivalente:

1) Există $a \in \mathbf{R}$ astfel încît $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$;

2) $AX = XA$ oricare ar fi $X \in M_2(\mathbf{R})$.

8. 1) Determinați matricele $A \in M_2(\mathbf{Z})$ cu proprietățile:

$$A^2 = E \text{ și } \det(A) = 1.$$

2) Dacă

$$B = \begin{pmatrix} a & 1 + a \\ 1 - a & -a \end{pmatrix},\ a \in \mathbf{Z},$$

arătați că $B^2 = E$ și $\det(B) = -1$.

9. Pentru orice $a \in \mathbf{R}$ fie matricele $U_a, V_a \in M_2(\mathbf{R})$,

$$U_a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix},\quad V_a = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}.$$

Arătați că:

1) $U_a U_b = U_{a+b}$, $V_a V_b = V_{a+b}$, $\forall a, b \in \mathbf{R}$;

2) $U_a U_{-a} = U_{-a} U_a = E$, $V_a V_{-a} = V_{-a} V_a = E$, $\forall a \in \mathbf{R}$.

10. Dacă $A \in M_2(\mathbf{R})$, $A = (a_{ij})$, atunci definim matricea

$${}^T A = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix} \in M_2(\mathbf{R})$$

numită *transpusa* matricei A. Verificați că:

1) ${}^T(A + B) = {}^T A + {}^T B$,

2) ${}^T(AB) = {}^T B\, {}^T A$

3) ${}^T({}^T A) = A$

oricare ar fi $A, B \in M_2(\mathbf{R})$.

4) Funcția $f : M_2(\mathbf{R}) \to M_2(\mathbf{R})$, $f(A) = {}^T A$, $A \in M_2(\mathbf{R})$ este bijectivă.

11. Fie $H = \left\{ A \in M_2(\mathbf{R}) \;\middle|\; A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix},\ a,\ b \in \mathbf{R},\ a \neq 0 \right\}$.

Arătați:

1) Dacă $A, B \in H$, atunci $AB \in H$.

2) Oricare ar fi $A \in H$ există $X \in H$ astfel încît $AX = E$.

Comparați rezultatele acestui exercițiu cu cele de la Ex. 3.

12. Fie $a, b_1, b_2, \ldots, b_n \in \mathbf{Z}$. Demonstrați:

1) Dacă $(a, b_i) = 1$, $1 \leqslant i \leqslant n$, atunci $(a, b_1 b_2 \ldots b_n) = 1$;

2) Dacă pentru orice $i \neq j$ avem $(b_i, b_j) = 1$ și $b_i \mid a$, $1 \leqslant i \leqslant n$, atunci $b_1 b_2 \ldots b_n$ divide pe a.

13. Dacă n este impar, arătați că $n^5 - n$ se divide prin 240.

14. 1) Determinați numerele $v \in \mathbf{Z}[\sqrt{-5}]$, $v = a + b\sqrt{-5}$, $a, b \in \mathbf{Z}$, cu proprietatea că există $z \in \mathbf{Z}[\sqrt{-5}]$ astfel încît $vz = 1$.

2) Găsiți $z \in \mathbf{Q}(\sqrt{-5})$ astfel încît $vz = 1$, unde $v = 3 - \sqrt{-5}$.

* * *

15*. Fie E o mulțime și $C_E : \mathfrak{P}(E) \to \mathfrak{P}(E)$, $C_E(X) = E \setminus X$, $\forall X \in \mathfrak{P}(E)$. Arătați că aplicația C_E are proprietățile:

1) $C_E(X \cup Y) = C_E(X) \cap C_E(Y)$ $\forall X, Y \in \mathfrak{P}(E)$,

2) $C_E(X \cap Y) = C_E(X) \cup C_E(Y)$ $\forall X, Y \in \mathfrak{P}(E)$,

3) $C_E \circ C_E = 1_{\mathfrak{P}(E)}$,

4) Aplicația C_E este bijectivă.

16*. Fie $A \in M_2(\mathbf{R})$, $A = (a_{ij})$, $E = \mathbf{R} \times \mathbf{R}$ și $f_A : E \to E$,

$f_A(x) = (a_{11}x_1 + a_{12}x_2,\ a_{21}x_1 + a_{22}x_2)$ $\forall x = (x_1, x_2) \in E$.

Arătați că următoarele afirmații sînt echivalente:

1) f_A este bijectivă;

2) $\det(A) \neq 0$.

17*. Pentru orice $A \in M_2(\mathbf{R})$, $A=(a_{ij})$ definim aplicația f_A ca la Ex. 16*. Arătați că:

1) $f_A = f_B \Leftrightarrow A = B$;

2) $f_A \circ f_B = f_{AB}$, $\forall A, B \in M_2(\mathbf{R})$;

3) Folosind asociativitatea compunerii funcțiilor, deduceți că $(AB)C = A(BC)$, $\forall A, B, C \in M_2(\mathbf{R})$.

18*. Determinați matricele $A \in M_2(\mathbf{Z})$ cu proprietatea: $A^2 = -E$.

19*. Fie $O_2 = \{A \in M_2(\mathbf{R}) \mid {}^tAA = E\}$. Arătați:

1) Dacă $A \in O_2$, atunci $\det(A) = \pm 1$;

2) Avem $A \in O_2$ și $\det(A) = 1 \Leftrightarrow \exists \theta \in [0, 2\pi)$ astfel încît

$$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

3) Avem $A \in O_2$ și $\det(A) = -1 \Leftrightarrow \exists \theta \in [0, 2\pi)$ astfel încît

$$A = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

4) Avem $A \in O_2 \Leftrightarrow {}^tAA = A^tA = E$;

5) Dacă $A, B \in O_2 \Rightarrow AB \in O_2$.

20*. Fie $\mathcal{K} = \{A \in M_2(\mathbf{R}) \mid {}^tA = A\}$ și $\mathcal{S} = \{A \in M_2(\mathbf{R}) \mid {}^tA = -A\}$.

Arătați că:

1) $\forall A, B \in \mathcal{K} \Rightarrow A + B \in \mathcal{K}$;

2) $\forall A, B \in \mathcal{S} \Rightarrow A + B \in \mathcal{S}$;

3) $A \in \mathcal{K} \cap \mathcal{S} \Rightarrow A = 0$;

4) $\forall A \in M_2(\mathbf{R})$ există $B \in \mathcal{K}$ și $C \in \mathcal{S}$ unic determinate cu proprietatea $A = B + C$.

21*. Dacă numerele $a, b, q, r \in \mathbf{Z}$ satisfac relația $a = bq + r$, atunci $(a, b) = (b, r)$. Deduceți că (a, b) este egal cu ultimul rest diferit de 0 din algoritmul lui Euclid pentru a și b.

22*. Fie a și b două numere întregi nenegative.

1) Arătați că $(2^a - 1, 2^b - 1) = 2^{(a,b)} - 1$;

2) Deduceți că $(2^a - 1, 2^b - 1) = 1 \Leftrightarrow (a, b) = 1$.

23*. Fie $q \in \mathbf{Z}$, $q > 0$ astfel încît $q - 3$ nu se divide prin 5. Dacă $m_1 = 2^{6q-1} - 1$, $m_2 = 2^{6q+1} - 1$, $m_3 = 2^{6q+3} - 1$, $m_4 = 2^{6q+3} - 1$, $m_5 = 2^{6q+5} - 1$, $m_6 = 2^{6q+7} - 1$, atunci $(m_i, m_j) = 1$ pentru $i \neq j$.

24*. Fie $f : \mathbf{Z}[\sqrt{2}] \to M_2(\mathbf{Z})$,

$$f(z) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \quad \forall z \in \mathbf{Z}[\sqrt{2}], \quad z = a + b\sqrt{2}.$$

Arătați că:

1) $f(z + w) = f(z) + f(w)$, $\forall z, w \in \mathbf{Z}[\sqrt{2}]$;

2) $f(zw) = f(z)f(w)$, $\forall z, w \in \mathbf{Z}[\sqrt{2}]$.

Capitolul II — LEGI DE COMPOZIȚIE

§ 1. NOȚIUNEA DE LEGE DE COMPOZIȚIE. EXEMPLE

Să trecem mai întîi în revistă cîteva exemple cunoscute care permit degajarea conceptului de lege de compoziție.

Pentru moment să ne fixăm atenția asupra mulțimii $\mathbf{N} = \{0, 1, 2, \ldots, n, \ldots\}$ a numerelor naturale. Operația de *adunare* a numerelor naturale ne permite să definim aplicația

$$\varphi : \mathbf{N} \times \mathbf{N} \to \mathbf{N}, \ (x, y) \to \varphi(x, y)$$

prin care facem să corespundă la orice pereche ordonată (x, y) de numere naturale un număr natural unic determinat $\varphi(x, y) = x + y$, numit *suma* lui x cu y. Astfel, $\varphi(3, 7) = 3 + 7 = 10$, $\varphi(5, 4) = 5 + 4 = 9$ etc.

Analog, folosind *înmulțirea* numerelor naturale, putem defini aplicația

$$\psi : \mathbf{N} \times \mathbf{N} \to \mathbf{N}, \ (x, y) \to \psi(x, y)$$

prin care la orice pereche ordonată (x, y) de numere naturale asociem un număr natural unic determinat $\psi(x, y) = xy$, numit *produsul* lui x cu y. Astfel $\psi(3, 7) = 3 \times 7 = 21$, $\psi(5, 4) = 5 \times 4 = 20$ etc.

Schimbînd cadrul, observații similare pot fi făcute pe mulțimea $\mathcal{P}(E)$ a tuturor părților X ale unei mulțimi date E. Putem defini aplicațiile:

$$\varphi : \mathcal{P}(E) \times \mathcal{P}(E) \to \mathcal{P}(E), \ (X, Y) \to \varphi(X, Y) = X \cup Y$$

și

$$\psi : \mathcal{P}(E) \times \mathcal{P}(E) \to \mathcal{P}(E), \ (X, Y) \to \psi(X, Y) = X \cap Y.$$

În viziunea aceasta, φ poartă numele de operație de *reuniune* iar $\varphi(X, Y) = X \cup Y$ se numește *reuniunea* lui X cu Y; ψ poartă numele de operație de *intersecție* iar $\psi(X, Y) = X \cap Y$ se numește *intersecția* lui X cu Y.

Pentru a surprinde într-o schemă generală situații ca cele enumerate mai sus, vom considera o mulțime nevidă M și o aplicație

$$\varphi : M \times M \to M, \ (x, y) \to \varphi(x, y),$$

ignorînd natura elementelor mulțimii M, precum și regula efectivă prin care la orice pereche ordonată (x, y) de elemente din M se asociază un element unic $\varphi(x, y) \in M$. Se obține astfel noțiunea de *lege de compoziție* pe mulțimea M. Mai precis:

1.1. *Definiție.* **Fie M o mulțime nevidă. O aplicație φ definită pe produsul cartezian $M \times M$ cu valori în M,**

$$\varphi : M \times M \to M, \ (x, y) \to \varphi(x, y)$$

se numește *lege de compoziție* **pe M.**

Elementul unic determinat $\varphi(x, y) \in M$ care corespunde perechii ordonate $(x, y) \in M \times M$ prin aplicația φ se numește *compusul* lui x cu y prin legea de compoziție φ.

O lege de compoziție pe o mulțime M poartă încă numele de *operație algebrică* pe M sau *operație binară* pe M. Este clar că adunarea și înmulțirea numerelor naturale sînt legi de compoziție pe $M = \mathbb{N}$, reuniunea și intersecția sînt legi de compoziție pe mulțimea $M = \mathfrak{P}(E)$ a tuturor părților unei mulțimi E.

Legile de compoziție sînt date în diferite notații. De regulă se folosește fie notația *additivă*, fie notația *multiplicativă*. În notația *additivă* punem $\varphi(x, y) = x + y$. Elementul $x + y$ se numește *suma* lui x cu y, iar legea de compoziție φ se numește *adunare*. În notația *multiplicativă* punem $\varphi(x, y) = xy$ sau $\varphi(x, y) = x \cdot y$. Elementul xy se numește *produsul* lui x cu y, iar legea de compoziție φ se numește *înmulțire*.

În unele cazuri, fie obligați de tradiție, fie din necesitatea de a distinge între mai multe operații algebrice, pentru compusul $\varphi(x, y)$ al lui x cu y se folosesc încă notații ca:

$$x \circ y,\ x \wedge y,\ x \vee y,\ x * y,\ x \oplus y,\ x \perp y,\ x \top y,\ x \Delta y \text{ etc.}$$

Exemple

1. *Adunarea și înmulțirea matricelor.* Fie $M_2(\mathbb{R})$ mulțimea matricelor pătratice de ordin 2 cu coeficienți din $\mathbb{R}$.

   Asociind la fiecare pereche ordonată (A, B) de matrice din $M_2(\mathbb{R})$ matricea $A + B \in M_2(\mathbb{R})$ se obține o lege de compoziție φ pe $M_2(\mathbb{R})$,

   $$\varphi : M_2(\mathbb{R}) \times M_2(\mathbb{R}) \to M_2(\mathbb{R}),\ (A, B) \to \varphi(A, B) = A + B,$$

   numită *operația de adunare* a matricelor.

   Asociind la fiecare pereche ordonată (A, B) de matrice din $M_2(\mathbb{R})$ matricea $AB \in M_2(\mathbb{R})$ se obține o lege de compoziție ψ pe $M_2(\mathbb{R})$,

   $$\psi : M_2(\mathbb{R}) \times M_2(\mathbb{R}) \to M_2(\mathbb{R}),\ (A, B) \to \psi(A, B) = AB,$$

   numită *operația de înmulțire* a matricelor.

2. *Compunerea funcțiilor.* Fie E o mulțime și $\mathfrak{F}(E)$ mulțimea tuturor funcțiilor $f : E \to E$. Asociind la fiecare pereche ordonată (f, g) de funcții din $\mathfrak{F}(E)$ funcția $f \circ g \in \mathfrak{F}(E)$ se obține o lege de compoziție φ pe $\mathfrak{F}(E)$,

   $$\varphi : \mathfrak{F}(E) \times \mathfrak{F}(E) \to \mathfrak{F}(E),\ (f, g) \to \varphi(f, g) = f \circ g,$$

   numită *operația de compunere* a funcțiilor.

3. *Adunarea și înmulțirea modulo n.* Fie $\mathbf{Z}$ mulțimea numerelor întregi și $n > 0$ un număr întreg fixat. Este știut că pentru orice $a \in \mathbf{Z}$ există $q, r \in \mathbf{Z}$ unic determinați astfel încît

   $$a = nq + r,\ 0 \leqslant r < n.$$

Numărul r de mai sus, cunoscut sub numele de *restul* împărțirii lui a prin n, va fi notat cu $a \bmod n$ (se citește „a modulo n") și se numește încă *redusul modulo n* al numărului întreg a. Astfel, dacă $n = 5$, atunci $13 \bmod 5 = 3$, $(-8) \bmod 5 = 2$, $4 \bmod 5 = 4$.

Dacă $a, b \in \mathbf{Z}$ atunci definim *suma modulo n* a lui a cu b, notată cu $a \oplus b$, și *produsul modulo n* al lui a cu b, notat cu $a * b$, prin:

$$a \oplus b \overset{\text{def}}{=} (a + b) \bmod n,$$

respectiv

$$a * b \overset{\text{def}}{=} (ab) \bmod n.$$

Avem astfel pe $\mathbf{Z}$, alături de adunarea și înmulțirea uzuală

$$\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z},\ (a, b) \to a + b \text{ și } \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z},\ (a, b) \to ab,$$

următoarele două legi de compoziție:

$$\varphi : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z},\ (a, b) \to \varphi(a, b) = a \oplus b$$

și

$$\psi : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z},\ (a, b) \to \psi(a, b) = a * b$$

numite *adunarea modulo n*, respectiv *înmulțirea modulo n*.

Astfel, dacă $n = 6$, atunci $7 \oplus 9 = 4$, $(-3) * 5 = 3$ căci $7 \oplus 9 = (7 + 9) \bmod 6 = 16 \bmod 6 = 4$, $(-3) * 5 = ((-3) \times 5) \bmod 6 = (-15) \bmod 6 = 3$.

§ 2. PARTE STABILĂ. LEGE DE COMPOZIȚIE INDUSĂ

2.1. *Definiție.* **Fie M o mulțime pe care este dată o lege de compoziție φ. O submulțime H a lui M cu proprietatea:**

$$\forall x, y \in H \Rightarrow \varphi(x, y) \in H$$

se numește parte *stabilă* a lui M în raport cu legea de compoziție φ.

Dacă H este o parte stabilă a lui M în raport cu legea de compoziție $\varphi : M \times M \to M$, atunci pe H putem defini legea de compoziție $\varphi' : H \times H \to H$, punînd

$$\varphi'(x, y) \overset{\text{def}}{=} \varphi(x, y) \in H \qquad \forall x, y \in H.$$

Vom spune că φ' este *legea de compoziție indusă* pe H de către φ.

Exemple

1. Mulțimea $2\mathbf{Z} = \{2k \mid k \in \mathbf{Z}\}$ a numerelor întregi pare este o parte stabilă a lui $\mathbf{Z}$ în raport cu operația de adunare a numerelor întregi pentru că suma a două numere pare este un număr par.

În adevăr, dacă $x, y \in 2\mathbf{Z}$, $x = 2h$, $y = 2k$, atunci $x + y = 2h + 2k = 2(h + k) \in 2\mathbf{Z}$.

Mulțimea $2\mathbf{Z} + 1 = \{2k + 1 \mid k \in \mathbf{Z}\}$ a numerelor întregi impare este o parte stabilă a lui $\mathbf{Z}$ în raport cu înmulțirea și nu este parte stabilă a lui $\mathbf{Z}$ în raport cu adunarea. În adevăr, dacă $x, y \in 2\mathbf{Z} + 1$, atunci $x = 2h + 1$, $y = 2k + 1$, deci

$$xy = (2h + 1)(2k + 1) = 2(2hk + h + k) + 1 \in 2\mathbf{Z} + 1$$

și

$$x + y = 2h + 1 + 2k + 1 = 2(h + k + 1) \notin 2\mathbf{Z} + 1.$$

2. Fie n un număr natural mai mare ca 0 și

$$\mathcal{R}_n = \{0, 1, 2, \ldots, n - 1\} \subset \mathbf{Z}.$$

Mulțimea $\mathcal{R}_n$ este o parte stabilă a lui $\mathbf{Z}$ atît în raport cu adunarea modulo n cît și în raport cu înmulțirea modulo n. În adevăr, oricare ar fi $x, y \in \mathbf{Z}$ avem $x \oplus y \in \mathcal{R}_n$ și $x * y \in \mathcal{R}_n$ și în particular

$$\forall x, y \in \mathcal{R}_n \Rightarrow x \oplus y \in \mathcal{R}_n, \qquad x * y \in \mathcal{R}_n.$$

Dacă $n > 1$, atunci $\mathcal{R}_n$ nu este stabilă în raport cu adunarea numerelor întregi iar dacă $n > 2$, atunci $\mathcal{R}_n$ nu este stabilă în raport cu înmulțirea uzuală a numerelor întregi.

3. Fie $E = \{1, 2, 3\}$ și $H = \{f \in \mathcal{F}(E) \mid f(3) = 3\}$.

Atunci H este o parte stabilă a lui $\mathcal{F}(E)$ în raport cu operația de compunere. În adevăr, dacă $f, g \in H$, atunci $f(3) = 3$, $g(3) = 3$, deci

$$(f \circ g)(3) = f(g(3)) = f(3) = 3,$$

de unde $f \circ g \in H$.

§ 3. TABLA UNEI LEGI DE COMPOZIȚIE

Fie M o mulțime finită, $M = \{a_1, a_2, \ldots, a_n\}$. În acest caz o lege de compoziție φ pe M, $\varphi : M \times M \to M$, poate fi dată prin ceea ce este cunoscut sub numele de *tabla* operației φ, care constă dintr-un tabel cu n linii și n coloane afectate celor n elemente ale lui M. Tabla legii de compoziție φ conține la intersecția liniei lui a_i cu coloana lui a_j elementul $\varphi(a_i, a_j)$.

	a_1	a_2	...	a_j	...	a_n
a_1						
a_2						
⋮						
a_i				$\varphi(a_i, a_j)$		
⋮						
a_n						

Tabla unei operații este utilă în perfectarea calculelor algebrice și, așa cum se va vedea mai tîrziu, în testarea unor proprietăți ale operației.

Tablele operațiilor induse pe $\mathcal{R}_5 = \{0, 1, 2, 3, 4\}$ de adunarea și înmulțirea modulo 5 sînt următoarele:

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Tabla adunării modulo 5.

$*$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Tabla înmulțirii modulo 5.

Fie acum $E = \{1, 2, \ldots, n\}$. O funcție $f : E \to E$ se dă uneori cu ajutorul unui tabel cu două linii:

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}.$$

În prima linie se trec în ordine numerele 1, 2, ..., n iar în a doua linie se trec imaginile acestora prin f, anume $f(1), f(2), \ldots, f(n)$. Astfel, dacă $E = \{1, 2\}$, atunci elementele lui $\mathcal{F}(E)$ sînt:

$$e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}.$$

Tabla operației de compunere a funcțiilor din $\mathcal{F}(E)$ este următoarea:

$\circ$	e	f	g	h
e	e	f	g	h
f	f	e	h	g
g	g	g	g	g
h	h	h	h	h

Astfel, $f \circ h = g$. În adevăr

$$(f \circ h)(1) = f(h(1)) = f(2) = 1 = g(1)$$

și

$$(f \circ h)(2) = f(h(2)) = f(2) = 1 = g(2)$$

de unde $f \circ h = g$. Rezultă că la intersecția liniei lui f cu coloana lui h din tabla operației de compunere a funcțiilor din $\mathcal{F}(E)$ se pune funcția g.

Direct din tabla operației de compunere a funcțiilor din $\mathcal{F}(E)$ se deduce că submulțimea $H = \{e, f\}$ a lui $\mathcal{F}(E)$ este stabilă în raport cu operația de compunere a funcțiilor.

§ 4. ASOCIATIVITATE

Noțiunea de lege de compoziție prezintă un mare grad de generalitate. În definiția unei legi de compoziție φ pe o mulțime M se ignoră atît natura elementelor mulțimii M cît și modul efectiv în care φ acționează pe $M \times M$. Singura restricție pusă este ca φ să asocieze la orice cuplu ordonat (x, y) de elemente din M un element $\varphi(x, y)$ din M și numai unul. Din acest motiv studiul legilor de compoziție bazat doar pe definiția lor este foarte sărac în rezultate. S-a dovedit fertilă ideea de a studia legi de compoziție ce au proprietăți care pot fi „semnalate" în multe exemple „concrete".

Vom presupune în continuare că M este o mulțime nevidă echipată cu o lege de compoziție „$*$",

$$M \times M \to M, \ (x, y) \to x * y.$$

Expresia $x * y$ se citește: x compus cu y sau x star y sau x stea y.

Definițiile și rezultatele vor fi date folosind această notație (notația „star") urmînd să fie făcute precizările ce se impun și în alte notații pentru legea de compoziție.

Fie $x, y, z \in M$. Prezența parantezelor în expresia

$$(x * y) * z$$

cere următoarea procedură de calcul: se află întîi compusul lui x cu y și apoi $x * y$ se compune (la dreapta!) cu z, obținîndu-se în final elementul $(x * y) * z \in M$. Prezența parantezelor în expresia $x * (y * z)$ impune să aflăm întîi $y * z$ și să-l compunem apoi (la stînga!) cu x, obținîndu-se astfel elementul $x * (y * z) \in M$.

4.1. *Definiție.* **O lege de compoziție** $M \times M \to M$, $(x, y) \to x * y$, **se numește** *asociativă* **dacă:**

$$(x * y) * z = x * (y * z), \quad \forall x, y, z \in M.$$

Dacă legea de compoziție este dată în notație aditivă (multiplicativă) atunci proprietatea de asociativitate a acesteia se scrie:

$$(x + y) + z = x + (y + z), \quad \forall x, y, z \in M,$$

respectiv

$$(xy)z = x(yz), \quad \forall x, y, z \in M.$$

Dacă folosim notația $x \perp y$ pentru compusul lui x cu y, atunci proprietatea de asociativitate se scrie:

$$(x \perp y) \perp z = x \perp (y \perp z), \quad \forall x, y, z \in M.$$

Exemple

1. Adunarea și înmulțirea numerelor reale sînt legi de compoziție asociative pentru că

$$(x + y) + z = x + (y + z), \quad (xy)z = x(yz), \quad \forall x, y, z \in \mathbb{R}.$$

2. Adunarea și înmulțirea matricelor din $M_2(\mathbb{R})$ sînt legi de compoziție asociative, căci

$$(A + B) + C = A + (B + C), \quad (AB)C = A(BC), \quad \forall A, B, C \in M_2(\mathbb{R}).$$

3. Reuniunea și intersecția părților unei mulțimi E sînt legi de compoziție asociative, căci

$$(X \cup Y) \cup Z = X \cup (Y \cup Z), \qquad (X \cap Y) \cap Z = X \cap (Y \cap Z)$$

oricare ar fi $X, Y, Z \in \mathcal{P}(E)$.

4. Compunerea funcțiilor unei mulțimi E în ea însăși este o lege de compoziție asociativă, căci

$$(f \circ g) \circ h = f \circ (g \circ h), \qquad \forall f, g, h \in \mathcal{F}(E).$$

5. Pe mulțimea $\mathbb{Z}$ a numerelor întregi definim legea de compoziție

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \qquad (x, y) \to x - y.$$

Cum $(3 - 7) - 1 = -5 \neq -3 = 3 - (7 - 1)$, rezultă că această lege de compoziție nu este asociativă.

§ 5. COMUTATIVITATE

Proprietatea de asociativitate lărgește mult aria posibilităților în perfectarea calculului algebric. O altă sursă în acest sens este dată de legile de compoziție pentru care compusul a două elemente oarecare este independent de ordinea în care se face compunerea acestora. Mai precis:

5.1. *Definiție.* **O lege de compoziție** $M \times M \to M$, $(x, y) \to x * y$ **se numește** *comutativă*, **dacă:**

$$x * y = y * x, \qquad \forall x, y \in M.$$

Adunarea și înmulțirea numerelor reale, reuniunea și intersecția părților unei mulțimi sînt legi de compoziție comutative.

Observație. Comutativitatea unei legi de compoziție dată pe o mulțime finită M poate fi verificată pe tabla operației: elementul xy de la intersecția liniei lui x cu coloana lui y trebuie să fie egal cu elementul yx de la intersecția liniei lui y cu coloana lui x,

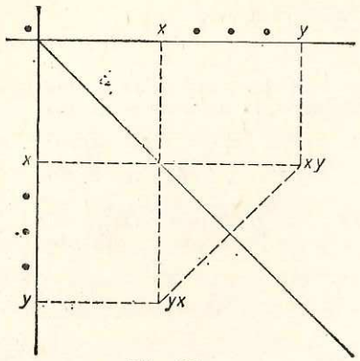


Fig. II.1

oricare ar fi $x, y \in M$. Aceasta revine la proprietatea că tabla operației este simetrică în raport cu diagonala principală (fig. II.1).

În § 8 au fost date tablele adunării și înmulțirii modulo 5 pe $\mathcal{A}_5 = \{0, 1, 2, 3, 4\}$. Cum aceste table sînt simetrice în raport cu diagonala principală, rezultă că legile de compoziție menționate sînt comutative. Tot la locul citat a fost dată tabla compunerii funcțiilor din $\mathcal{F}(E)$, unde $E = \{1, 2\}$. Pe tabla acestei legi de compoziție se constată că $h \circ g = h \neq g = g \circ h$, deci această operație nu este comutativă.

Numeroase legi de compoziție se definesc cu ajutorul altora deja cunoscute. Asemenea operații pot prelua unele proprietăți de la cele de plecare prin „mecanismul" dat chiar de definiția lor. Astfel comutativitatea adunării matricelor din $M_2(\mathbf{R})$ este o consecință a proprietății de comutativitate a adunării numerelor reale. În adevăr, dacă $A, B \in M_2(\mathbf{R})$, $A = (a_{ij})$, $B = (b_{ij})$, atunci

$$A + B = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix} =$$

$$= \begin{pmatrix} b_{11} + a_{11} & b_{12} + a_{12} \\ b_{21} + a_{21} & b_{22} + a_{22} \end{pmatrix} = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} + \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = B + A.$$

Să observăm că înmulțirea matricelor din $M_2(\mathbf{R})$ nu este comutativă, cu toate că înmulțirea numerelor reale este comutativă. Aceasta rezultă din exemplul următor:

$$\begin{pmatrix} 1 & 2 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ -1 & 0 \end{pmatrix}.$$

Exerciții rezolvate

R—1 Pe mulțimea $\mathbf{Z}$ a numerelor întregi definim legea de compoziție

$$\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}, \quad (x, y) \to x \circ y \overset{\text{def}}{=} x + y - xy,$$

numită *compunerea circulară*. Să se arate că legea de compoziție „$\circ$" este asociativă și comutativă.

Soluție. Dacă $x, y, z \in \mathbf{Z}$, atunci:

$$(x \circ y) \circ z = (x + y - xy) \circ z = x + y - xy + z - (x + y - xy)z =$$
$$= x + y + z - xy - yz - zx + xyz$$

$$x \circ (y \circ z) = x \circ (y + z - yz) = x + y + z - yz - x(y + z - yz) =$$
$$= x + y + z - xy - yz - zx + xyz,$$

de unde

$$(x \circ y) \circ z = x \circ (y \circ z).$$

De asemenea, pentru $x, y \in \mathbf{Z}$ avem:

$$x \circ y = x + y - xy = y + x - yx = y \circ x.$$

R—2 Fie M și N două mulțimi, „$*$" o lege de compoziție pe M, „$\circ$" o lege de compoziție pe N și $f : M \to N$ o funcție surjectivă astfel încît

$$f(x * y) = f(x) \circ f(y), \qquad \forall x, y \in M.$$

1) Dacă legea de compoziție „$*$" este asociativă (comutativă) atunci legea de compoziție „$\circ$" este asociativă (resp. comutativă).

2) Funcția $f : \mathbf{Z} \to \mathbf{Z}$, $f(x) = 1 - x$ are proprietatea

$$f(xy) = f(x) \circ f(y), \qquad \forall x, y \in \mathbf{Z}$$

unde xy este produsul uzual în $\mathbf{Z}$ iar „$\circ$" este compunerea circulară (v. Ex. R—1).

3) Dați o nouă soluție pentru Ex. R—1.

Soluție. 1) Fie $u, v, w \in N$. Cum f este funcție surjectivă, există $x, y, z \in M$ astfel încît $u = f(x)$, $v = f(y)$, $w = f(z)$.

Avem:

$$u \circ v = f(x) \circ f(y) = f(x * y) = f(y * x) = f(y) \circ f(x) = v \circ u$$

și

$$(u \circ v) \circ w = (f(x) \circ f(y)) \circ f(z) = f(x * y) \circ f(z) = f((x * y) * z) =$$
$$= f(x * (y * z)) = f(x) \circ f(y * z) = f(x) \circ (f(y) \circ f(z)) = u \circ (v \circ w).$$

2) Oricare ar fi $x, y \in \mathbf{Z}$ avem:

$$f(x) \circ f(y) = f(x) + f(y) - f(x)f(y) = 1 - x + 1 - y - (1 - x)(1 - y) =$$
$$= 1 - xy = f(xy).$$

3) Funcția f este surjectivă iar înmulțirea uzuală a numerelor întregi este asociativă și comutativă. Putem aplica 1).

5.4. *Observație.* Fie $\varphi : M \times M \to M$ o lege de compoziție pe M, H o parte stabilă a lui M în raport cu φ și φ' legea de compoziție pe H indusă de φ.

Dacă φ este asociativă (comutativă) atunci φ' este asociativă (respectiv comutativă). În adevăr, pentru orice $x, y, z \in H$ avem:

$$\varphi'(\varphi'(x, y), z)) = \varphi(\varphi(x, y), z)) = \varphi(x, \varphi(y, z)) = \varphi'(x, \varphi'(y, z))$$

și

$$\varphi'(x, y) = \varphi(x, y) = \varphi(y, x) = \varphi'(y, x).$$

Numerele reale 0 și 1 au proprietățile:

$$0 + x = x + 0 = x, \qquad \forall x \in \mathbf{R},$$

respectiv

$$1 \cdot x = x \cdot 1 = x, \qquad \forall x \in \mathbf{R}.$$

Dacă E este o mulțime și $1_E : E \to E$ este aplicația identică a lui E, atunci

$$1_E \circ f = f \circ 1_E = f, \qquad \forall f \in \mathcal{F}(E).$$

De asemenea, pentru orice $A \in M_2(\mathbf{R})$ avem:

$$0 + A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} 0 + a_{11} & 0 + a_{12} \\ 0 + a_{21} & 0 + a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = A$$

și analog $A + 0 = A$.

6.1. *Definiție.* **Un element $e \in M$ se numește *element neutru* pentru o lege de compoziție $M \times M \to M$, $(x, y) \to x * y$, dacă**

$$e * x = x * e = x, \qquad \forall x \in M.$$

6.2. **Teoremă. Dacă o lege de compoziție are element neutru, atunci acesta este unic.**

Demonstrație. Fie e și e' două elemente neutre pentru o lege de compoziție $M \times M \to M$, $(x, y) \to x * y$. Avem $e * e' = e'$ căci e este element neutru. De asemenea, $e * e' = e$ căci și e' este element neutru, de unde $e = e'$.

Așadar, elementul neutru, în caz de există, este unic determinat.

În notație aditivă elementul neutru se notează de regulă cu 0 și se numește *elementul zero* iar în notația multiplicativă elementul neutru se notează cu 1 sau chiar cu e și poartă numele de *elementul unitate*. Avem:

$$0 + x = x + 0 = x, \qquad \forall x \in M,$$

respectiv

$$1 \cdot x = x \cdot 1 = x, \qquad \forall x \in M.$$

Exemple

1. Numărul real 0 este elementul neutru al adunării numerelor reale, numărul real 1 este elementul neutru al înmulțirii numerelor reale.
2. Aplicația identică 1_E a mulțimii E este elementul neutru al operației de compunere a funcțiilor din $\mathcal{F}(E)$.
3. Fie E o mulțime. Cum $\varnothing \cup X = X \cup \varnothing = X$ și $E \cap X = X \cap E = X$ oricare ar fi $X \in \mathcal{P}(E)$ rezultă că $\varnothing$ este elementul neutru al operației „$\cup$" iar E este elementul neutru al operației „$\cap$".

4. Mulțimea $2\mathbf{N} = \{2k \mid k \in \mathbf{N}\}$ a numerelor naturale pare este o parte stabilă a lui $\mathbf{N}$ în raport cu înmulțirea și legea de compoziție indusă de către aceasta pe $2\mathbf{N}$ nu admite element neutru.

§ 7. ELEMENTE SIMETRIZABILE

Ca și pînă acum, M este o mulțime nevidă înzestrată cu o lege de compoziție

$$M \times M \to M, \ (x, y) \to x * y$$

Vom presupune în plus că această lege de compoziție este asociativă și că admite element neutru, fie acesta e.

7.1. **Definiție. Un element $x \in M$ se numește *simetrizabil* în raport cu legea de compoziție (asociativă și cu element neutru) $M \times M \to M$, $(x, y) \to x * y$, dacă există $x' \in M$ astfel încît**

$$x' * x = x * x' = e.$$

Să observăm că dacă $x'' \in M$ satisface ca și x' condițiile

$$x'' * x = x * x'' = e,$$

atunci $x' = x''$. În adevăr

$$x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x''.$$

Dacă $x \in M$ este simetrizabil, atunci unicul element $x' \in M$ cu proprietatea $x' * x = x * x' = e$ se numește *simetricul* lui x (în raport cu operația „$*$").

În notația multiplicativă simetricul lui x, în caz că există, se notează de regulă cu x^{-1} și se numește *inversul* lui x; în notația aditivă se notează cu $-x$ și se numește *opusul* lui x. Așadar,

$$x^{-1}x = xx^{-1} = 1,$$

respectiv

$$(-x) + x = x + (-x) = 0.$$

Exemple

1. Cum $e * e = e$, rezultă că elementul neutru este simetrizabil și simetricul lui e este tot e. În notație multiplicativă avem $1^{-1} = 1$, iar în notație aditivă $-0 = 0$.
2. Matricea $A \in M_2(\mathbf{Z})$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ cu $ad - cb = 1$, este simetrizabilă (inversabilă) în raport cu operația de înmulțire din $M_2(\mathbf{Z})$ și

$$A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in M_2(\mathbf{Z}).$$

În adevăr,

$$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & -cb+ad \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E$$

și analog

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E.$$

3. Orice număr întreg este simetrizabil în raport cu adunarea numerelor întregi; numerele întregi simetrizabile față de înmulțire sînt 1 și -1, $1^{-1} = 1$, $(-1)^{-1} = -1$.

4. Consultînd tabla dată la §5 pentru compunerea funcțiilor din $\mathfrak{F}(E)$, unde $E = \{1, 2\}$, se observă că $e \circ e = e$ și $f \circ f = e$ deci funcțiile e și f sînt simetrizabile (inversabile) și $e^{-1} = e$, $f^{-1} = f$.

7.2. Teoremă. Dacă $x, y \in M$ sînt elemente simetrizabile în raport cu o lege de compoziție $M \times M \to M$, $(x, y) \to x * y$ (asociativă și cu element neutru) atunci $x * y$ și x' sînt simetrizabile. Mai mult:

1) $(x * y)' = y' * x'$,

2) $(x')' = x$.

Demonstrație. Avem:

$$(y' * x') * (x * y) = y' * (x' * (x * y)) = y' * ((x' * x) * y) =$$
$$= y' * (e * y) = y' * y = e$$

și analog $(x * y) * (y' * x') = e$. Rezultă că $x * y$ este simetrizabil și $(x * y)' = y' * x'$. A doua afirmație este imediată.

Proprietățile 1) și 2) din enunțul teoremei precedente se transcriu multiplicativ astfel:

$$(xy)^{-1} = y^{-1}x^{-1}, \quad (x^{-1})^{-1} = x,$$

iar în notația aditivă

$$-(x + y) = (-y) + (-x), \quad -(-x) = x.$$

Se face următoarea convenție de notație:

$$\boxed{x - y \overset{\text{def}}{=} x + (-y)}$$

Exerciții rezolvate

R—1 Să se arate că legea de compoziție

$$\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}, \quad (x, y) \to x \circ y = x + y - xy$$

are element neutru și să se determine elementele simetrizabile. Aceeași problematică pentru legea de compoziție

$$\mathbf{Q} \times \mathbf{Q} \to \mathbf{Q}, \quad (x, y) \to x \circ y = x + y - xy.$$

Soluție. Dacă $e \in \mathbf{Z}$ este element neutru pentru legea de compoziție „$\circ$", trebuie să avem

$$x = e \circ x = e + x - ex, \qquad \forall x \in \mathbf{Z}$$

deci

$$e = ex, \qquad \forall x \in \mathbf{Z}$$

și în particular $e = e \cdot 0 = 0$. Pe de altă parte se verifică că $0 \circ x = x \circ 0 = x$, $\forall x \in \mathbf{Z}$, deci numărul 0 este elementul neutru al legii de compoziție „$\circ$".

Fie $a \in \mathbf{Z}$. Pentru ca a să fie simetrizabil în raport cu legea de compoziție „$\circ$" trebuie să existe $x \in \mathbf{Z}$ astfel încît

$$0 = a \circ x = a + x - ax,$$

de unde

$$x(a - 1) = a.$$

Se observă că această ecuație admite o soluție $x \in \mathbf{Z}$ dacă și numai dacă $a = 0$ și $a = 2$. Elementele simetrizabile sînt 0 și 2, $0' = 0$ și $2' = 2$.

Cînd $\mathbf{Z}$ se înlocuiește cu $\mathbf{Q}$, elementele simetrizabile sînt toate numerele raționale $a \neq 1$.

R—2 Fie d un număr întreg liber de pătrate și

$$H = \left\{ A \in M_2(\mathbf{Q}) \,\middle|\, A = \begin{pmatrix} a & db \\ b & a \end{pmatrix},\ a, b \in \mathbf{Q},\ a \neq 0 \text{ sau } b \neq 0 \right\}$$

1) H este o parte stabilă a lui $M_2(\mathbf{Q})$ în raport cu înmulțirea matricelor.

2) Orice matrice $A \in H$ este inversabilă (simetrizabilă) în raport cu operația indusă.

Soluție. 1) Fie $A, B \in H$, $A = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}$, $B = \begin{pmatrix} a' & db' \\ b' & a' \end{pmatrix}$.

Avem:

$$AB = \begin{pmatrix} aa' + dbb' & d(ba' + ab') \\ ba' + ab' & aa' + dbb' \end{pmatrix} = \begin{pmatrix} a'' & db'' \\ b'' & a'' \end{pmatrix}$$

unde $a'' = aa' + dbb' \in \mathbf{Q}$, $b'' = ba' + ab' \in \mathbf{Q}$. Pentru a avea $AB \in H$ este suficient să arătăm că $a'' \neq 0$ sau $b'' \neq 0$. Dacă $a'' = 0$ și $b'' = 0$ atunci $x = a'$ și $y = b'$ este o soluție nebanală a sistemului omogen:

$$(*) \quad \begin{cases} ax + dby = 0, \\ bx + ay = 0. \end{cases}$$

Determinantul matricei acestui sistem este egal cu $a^2 - db^2$. Cum d este liber de pătrate și $a \neq 0$ sau $b \neq 0$, rezultă că $a^2 - db^2 \neq 0$ căci altfel $\sqrt{d} \in \mathbf{Q}$. Contradicție. Dar din $a^2 - db^2 \neq 0$ rezultă că singura soluție a sistemului (*) este $x = y = 0$. Rămîne adevărat că $a'' \neq 0$ sau $b'' \neq 0$, deci $AB \in H$.

2) Se observă că matricea unitate $E \in H$ și fie $A \in H$. Să arătăm că există o matrice $X \in H$,

$$X = \begin{pmatrix} x & dy \\ y & x \end{pmatrix}, \quad x, y \in \mathbf{Q},\ x \neq 0 \text{ sau } y \neq 0$$

astfel încît $XA = AX = E$. Avem:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E = AX = \begin{pmatrix} a & db \\ b & a \end{pmatrix}\begin{pmatrix} x & dy \\ y & x \end{pmatrix} = \begin{pmatrix} ax + dby & d(bx + ay) \\ bx + ay & ax + dby \end{pmatrix}$$

ceea ce este echivalent cu sistemul liniar:

$$(**) \quad \begin{cases} ax + dby = 1, \\ bx + ay = 0. \end{cases}$$

Determinantul sistemului (**) este $a^2 - db^2 \neq 0$ și unica soluție este $x = a/(a^2 - db^2)$, $y = -b/(a^2 - db^2)$.

Cum $a \neq 0$ sau $b \neq 0$, rezultă $x \neq 0$ sau $y \neq 0$. Așadar:

$$X = \begin{pmatrix} \dfrac{a}{a^2 - db^2} & \dfrac{-db}{a^2 - db^2} \\ \dfrac{-b}{a^2 - db^2} & \dfrac{a}{a^2 - db^2} \end{pmatrix} \in H.$$

Se verifică și egalitatea $XA = E$, deci A^{-1} există și $A^{-1} = X \in H$.

§ 8. PROPRIETĂȚI ALE ADUNĂRII ȘI ÎNMULȚIRII MODULO n

În capitolul *I*, § 1, au fost enumerate proprietățile adunării și înmulțirii numerelor întregi.

Anume, cu terminologia adoptată în capitolul de față, adunarea numerelor întregi,

$$\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}, \ (x, y) \to x + y$$

este asociativă, comutativă, admite pe 0 ca element neutru și orice număr întreg admite opus.

De asemenea, înmulțirea numerelor întregi

$$\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}, \ (x, y) \to xy,$$

este asociativă, comutativă și admite pe 1 ca element neutru.

În fine, înmulțirea numerelor întregi este *distributivă* față de adunare:

$$x(y + z) = xy + xz, \qquad \forall x, y, z \in \mathbf{Z}.$$

Fie $n > 0$ un număr întreg. Dacă $a, b \in \mathbf{Z}$ am definit *suma modulo n* a lui a cu b, notată cu $a \oplus b$ și *produsul modulo n* al lui a cu b, notat cu $a * b$ ca fiind restul împărțirii prin n al numărului $a + b$, respectiv ab:

$$a \oplus b \overset{\text{def}}{=} (a + b) \bmod n, \qquad a * b \overset{\text{def}}{=} (ab) \bmod n.$$

S-au obținut astfel două legi de compoziție pe $\mathbf{Z}$,

$$\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}, \ (a, b) \to a \oplus b \text{ și } \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}, \ (a, b) \to a * b$$

numite *adunarea modulo n*, respectiv *înmulțirea modulo n*.

Ne propunem în continuare să studiem proprietățile acestora. Un rezultat util pentru acest studiu este următorul:

8.1. **Lemă.** **Fie $a, b \in \mathbf{Z}$. Atunci oricare ar fi $h, k \in \mathbf{Z}$ avem:**

$$(a + nh) \oplus (b + nk) = a \oplus b$$

și

$$(a + nh) * (b + nk) = a * b.$$

Demonstrație. Pentru orice h și $k \in \mathbf{Z}$ avem:

$$(a + nh) + (b + nk) = (a + b) + n(h + k)$$

și

$$(a + nh)(b + nk) = ab + n(ak + bh + nhk)$$

Rezultă că numerele $(a + nh) + (b + nk)$ și $a + b$ dau același rest prin împărțirea cu n, deci

$$(a + nh) \oplus (b + nk) = a \oplus b$$

și, de asemenea, numerele $(a + nh)(b + nk)$ și ab dau același rest prin împărțirea cu n, deci

$$(a + nh) * (b + nk) = a * b.$$

8.2. **Teoremă.** **Operațiile de adunare și înmulțire modulo n au proprietățile:**

1) $(a \oplus b) \oplus c = a \oplus (b \oplus c)$,

2) $a \oplus b = b \oplus a$,

3) $(a * b) * c = a * (b * c)$,

4) $a * b = b * a$,

5) $a * (b \oplus c) = a * b \oplus a * c$.

oricare ar fi $a, b, c \in \mathbf{Z}$.

Demonstrație. Cum $a \oplus b$ este restul împărțirii lui $a + b$ prin n, există $q, \in \mathbf{Z}$ astfel încît

$$a + b = nq + (a \oplus b).$$

Din lema precedentă rezultă:

$$(a \oplus b) \oplus c = (a + b) \oplus c = ((a + b) + c) \bmod n.$$

Analog se arată că:

$$a \oplus (b \oplus c) = a \oplus (b + c) = (a + (b + c)) \bmod n.$$

Dar $(a + b) + c = a + (b + c)$, de unde $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

4) Avem:

$$a * b = (ab) \bmod n = (ba) \bmod n = b * a.$$

5) Aplicînd lema 8.1 avem:

$$a * (b \oplus c) = a * (b + c) = (a(b + c)) \bmod n = (ab + ac) \bmod n =$$
$$= ab \oplus ac = a * b \oplus a * c.$$

Proprietatea 2) se demonstrează ca 4), iar 3) ca 1).

Să observăm că adunarea modulo n nu admite element neutru. În adevăr, să presupunem că $0 \in \mathbf{Z}$ este astfel încît $0 \oplus a = a \oplus 0 = a$, $\forall a \in \mathbf{Z}$. Dacă $a \notin \mathcal{R}_n = \{0, 1, 2, \ldots, n-1\}$, atunci $0 \oplus a \neq a$ pentru că $0 \oplus a \in \mathcal{R}_n$. Contradicție.

Analog se arată că înmulțirea modulo n nu admite element neutru.

Așa cum s-a mai observat, avem:

$$\forall a, b \in \mathcal{R}_n \Rightarrow a \oplus b \in \mathcal{R}_n, \quad a * b \in \mathcal{R}_n.$$

Putem deci considera operațiile induse pe $\mathcal{R}_n$ de către operațiile de adunare și înmulțire modulo n,

$$\mathcal{R}_n \times \mathcal{R}_n \to \mathcal{R}_n, \qquad (a, b) \to a \oplus b$$

respectiv

$$\mathcal{R}_n \times \mathcal{R}_n \to \mathcal{R}_n, \qquad (a, b) \to a * b.$$

Aceste operații au evident proprietățile 1)—5) din enunțul Teoremei 8.2 (v. Obs. 5.4). Cum:

$$0 \oplus a = a \oplus 0 = a, \qquad 1 * a = a * 1 = a, \qquad \forall a \in \mathcal{R}_n$$

rezultă că numerele 0 și 1 sînt elemente neutre pentru operațiile induse pe $\mathcal{R}_n$ de către adunarea modulo n, respectiv înmulțirea modulo n.

În fine, să mai observăm că

$$a \oplus (n - a) = (n - a) \oplus a = 0, \qquad \forall a \in \mathcal{R}_n$$

și cum $n - a \in \mathcal{R}_n$ oricare ar fi $a \in \mathcal{R}_n$, rezultă că orice element $a \in \mathcal{R}_n$ este simetrizabil în raport cu operația indusă pe $\mathcal{R}_n$ de către adunarea modulo n, simetricul (opusul) lui a fiind $n - a$.

Fie $n = 6$. Tablele operațiilor induse pe $\mathcal{R}_6 = \{0, 1, 2, 3, 4, 5\}$ de către adunarea și înmulțirea modulo 6 sînt:

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Tabla adunării modulo 6

$*$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Tabla înmulțirii modulo 6

Faptul că operația indusă pe $\mathcal{R}_6$ de adunarea modulo 6 este comutativă și că admite pe 0 ca element neutru se constată și pe tabla acesteia. Folosind notația aditivă pentru simetric, se constată de asemenea că:

$$-0 = 0, \quad -1 = 5, \quad -2 = 4, \quad -3 = 3, \quad -4 = 2, \quad -5 = 1$$

căci

$$0 \oplus 0 = 0, \; 1 \oplus 5 = 0, \; 2 \oplus 4 = 0, \; 3 \oplus 3 = 0.$$

Elementele din $\mathcal{R}_6$ simetrizabile în raport cu operația indusă de înmulțirea modulo 6 sînt 1 și 5. Folosind în acest caz notația multiplicativă pentru simetric, avem:

$$1^{-1} = 1, \qquad 5^{-1} = 5$$

căci $1 * 1 = 1$, $5 * 5 = 1$.

Exerciții rezolvate

R — 1 Găsiți soluțiile din $\mathcal{R}_6$ ale ecuațiilor:

1) $5 * x \oplus 2 = 4$,
2) $3 * x \oplus 4 = 4$,
3) $2 * x \oplus 3 = 2$,

unde „$\oplus$" și „$*$" sînt simbolurile adunării și înmulțirii modulo 6.

Soluție. 1) Cum $5 * x \oplus 2 \oplus 4 = 4 \oplus 4$ iar $2 \oplus 4 = 0$ și $4 \oplus 4 = 2$, rezultă că

$$5 * x = 2.$$

Din tabla înmulțirii modulo 6 rezultă că $x = 4$. Același rezultat se obține observînd că 5 este simetrizabil în raport cu „$*$" și $5^{-1} = 5$. Deducem:

$$x = 1 * x = (5 * 5) * x = 5 * (5 * x) = 5 * 2 = 4.$$

2) Cum $3 * x \oplus 4 \oplus 2 = 4 \oplus 2$, rezultă că $3 * x = 0$.
Din tabla înmulțirii modulo 6, găsim pentru x valorile $x_1 = 0$, $x_2 = 2$ și $x_3 = 4$ (O ecuație de grad 1 admite trei soluții!).

3) Cum $2 * x \oplus 3 \oplus 3 = 2 \oplus 3$, rezultă $2 * x = 5$. Din tabla înmulțirii modulo 6 se constată că nu există $x \in \mathcal{R}_6$ astfel încît $2 * x = 5$. Așadar ecuația 3) nu admite soluții.

R — 2 1) Rezolvați în $\mathcal{R}_5$ ecuația $2 * x \oplus 3 = 2$.

2) Arătați că ecuația $a * x \oplus b = 0$ cu $a, b \in \mathcal{R}_5$, $a \neq 0$, admite o soluție unică în $\mathcal{R}_5$.

Soluție. 1) Adunînd la fiecare termen al ecuației opusul lui 3 în raport cu adunarea modulo 5 pe $\mathcal{R}_5$, se obține:

$$2 * x \oplus 3 \oplus 2 = 2 \oplus 2,$$

deci

$$2 * x = 4.$$

Din tabla înmulțirii modulo 5 pe $\mathcal{R}_5$ se constată că 2 este simetrizabil și simetricul lui 2 în raport cu această operație este 3. Înmulțind cu 3 ecuația $2 * x = 4$ se obține

$$3 * 2 * x = 3 * 4$$

și cum $3 * 2 = 1$, $3 * 4 = 2$, deducem că $x = 2$.

2) Consultînd tablele înmulțirii și adunării modulo 5 pe $\mathcal{R}_5 = \{0, 1, 2, 3, 4\}$ (v. § 3) se constată că toate elementele $b \in \mathcal{R}_5$ sînt simetrizabile în raport cu adunarea modulo 5 și că toate elementele $a \in \mathcal{R}_5$, $a \neq 0$, sînt simetrizabile în raport cu înmulțirea modulo 5. Așadar etapele de rezolvare de la pct. 1) pot fi parcurse și pe cazul general $a * x \oplus b = 0$ $a \neq 0$, deci ecuația $a * x \oplus b = 0$ are cel puțin o soluție în $\mathcal{R}_5$.

Fie $x_1, x_2 \in \mathcal{A}_5$ astfel încît $a * x_1 \oplus b = 0$ și $a * x_2 \oplus b = 0$. Atunci avem:

$$a * x_1 \oplus b = a * x_2 \oplus b.$$

Adunînd opusul lui b la fiecare termen al egalității precedente obținem

$$a * x_1 = a * x_2$$

și înmulțind termenii acestei ultime egalități cu simetricul lui a în raport cu înmulțirea modulo 5 se obține $x_1 = x_2$.

§ 9. SUME ȘI PRODUSE ITERATE

Fie M o mulțime nevidă înzestrată cu o lege de compoziție asociativă și cu element neutru,

$$M \times M \to M,\ (x,\ y) \to xy.$$

Fie $a \in M$. Definim inductiv *puterile* lui a cu exponenți numere naturale astfel:

$$a^0 = e,\ a^1 = a,\ a^2 = aa,\ a^3 = a^2a,\ \ldots,\ a^n = a^{n-1}\ a,\ \ldots,$$

sau mai condensat prin

$$a^n \overset{\text{def}}{=} \begin{cases} e & \text{dacă } n = 0, \\ a^{n-1} \cdot a & \text{dacă } n > 0. \end{cases}$$

9.1. *Teoremă.* **Oricare ar fi numerele naturale** m **și** n **avem:**

$$\boxed{a^m \cdot a^n = a^{m+n},\quad (a^m)^n = a^{mn}}$$

Demonstrație. Este suficient să arătăm că pentru m fixat, afirmațiile din enunț sînt adevărate oricare ar fi $n \in \mathbb{N}$. Cum

$$a^m \cdot a^0 = a^m \cdot e = a^m = a^{m+0}$$

și

$$(a^m)^0 = e = a^0 = a^{m \cdot 0},$$

afirmațiile din enunț sînt adevărate pentru $n = 0$.

Presupunem că $n > 0$ și că afirmațiile din enunț sînt adevărate pentru $n - 1$. Atunci:

$$a^m a^n = a^m(a^{n-1} \cdot a) = (a^m \cdot a^{n-1})a = a^{m+n-1}\ a = a^{m+n}$$

și

$$(a^m)^n = (a^m)^{n-1} \cdot a^m = a^{m(n-1)} \cdot a^m = a^{m(n-1)+m} = a^{mn}.$$

Analog, dacă legea de compoziție este dată aditiv, definim *multiplii na* ai lui a, cu $n \in \mathbb{N}$, astfel:

$$na \overset{\text{def}}{=} \begin{cases} 0 & \text{dacă } n = 0 \\ (n-1)a + a & \text{dacă } n > 0. \end{cases}$$

Rezultatul din teorema precedentă se transcrie aditiv astfel:

$$\boxed{ma + na = (m+n)a,\ n(ma) = (nm)a\ \forall m,\ n \in \mathbb{N}}$$

O lege de compoziție pe M dată în notație multiplicativă (aditivă) permite definirea produsului ab (respectiv sumei $a + b$) pentru oricare două elemente $a, b \in M$. Se poate defini inductiv *produsul* $\prod_{i=1}^{n} a_i$ (respectiv *suma* $\sum_{i=1}^{n} a_i$) unui număr finit de elemente $a_1, a_2, \ldots, a_n$ din M după cum urmează:

$$\prod_{i=}^{n} a_i \overset{\text{def}}{=} \begin{cases} a_1 & \text{dacă } n = 1 \\ \left(\prod_{i=1}^{n-1} a_i\right) a_n & \text{dacă } n > 1 \end{cases}$$

respectiv

$$\sum_{i=1}^{n} a_i \overset{\text{def}}{=} \begin{cases} a_1 & \text{dacă } n = 1, \\ \left(\sum_{i=1}^{n-1} a_i\right) + a_n & \text{dacă } n > 1. \end{cases}$$

Se mai folosesc notațiile:

$$a_1 a_2 \ldots a_n = \prod_{i=1}^{n} a_i,$$

respectiv

$$a_1 + a_2 + \ldots + a_n = \sum_{i=1}^{n} a_i.$$

Cînd legea de compoziție este asociativă, produsul (suma) unui număr finit de elemente este independent(ă) de gruparea factorilor (termenilor).

Exerciții rezolvate

R — 1 Fie $E = \{1, 2, 3, 4, 5\}$ și $f \in \mathcal{F}(E)$,

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 3 \end{pmatrix}.$$

1) Calculați $f^2 = f \circ f$, $f^3 = f^2 \circ f$, $f^4 = f^3 \circ f$, $f^5 = f^4 \circ f$ și deduceți că $f^2 = f^{2+3q}$ oricare ar fi $q = 0, 1, \ldots$.

2) Dacă $H = \{f^2, f^3, f^4\}$ arătați că $f^n \in H$ oricare ar fi $n \geqslant 2$.

3) Arătați că H este o parte stabilă a lui $\mathcal{F}(E)$ în raport cu compunerea funcțiilor. Alcătuiți tabla operației induse.

4) Deduceți că operația indusă pe H admite element neutru și că toate elementele lui H sînt simetrizabile în raport cu operația indusă.

Soluție. 1) Avem: $f^2 = f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 3 & 4 \end{pmatrix}$,

$f^3 = f^2 \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 4 & 5 \end{pmatrix}$, $f^4 = f^3 \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 5 & 3 \end{pmatrix}$, $f^5 = f^4 \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 3 & 4 \end{pmatrix} = f^2$.

Pentru $q = 0$ avem $f^{2+3\cdot 0} = f^2$, pentru $q = 1$ avem $f^{2+3\cdot 1} = f^5 = f^2$. Fie $q > 1$ și presupunem că $f^{2+3(q-1)} = f^2$. Atunci:

$$f^{2+3q} = f^{2+3(q-1)} \circ f^3 = f^2 \circ f^3 = f^5 = f^2.$$

2) Cum $n - 2 \geqslant 0$, există q, $r \in \mathbf{N}$ astfel încît $n - 2 = 3q + r$, $0 \leqslant r < 3$. Atunci

$$f^n = f^{2+3q+r} = f^{2+3q} \circ f^r = f^2 \circ f^r = f^{2+r} \in H$$

căci $2 \leqslant 2 + r < 5$.

3) Faptul că H este stabilă în raport cu compunerea rezultă din 2). De asemenea, folosind calculul de la 2) se alcătuiește tabla operației induse după cum urmează:

$\circ$	f^2	f^3	f^4
f^2	f^4	f^2	f^3
f^3	f^2	f^3	f^4
f^4	f^3	f^4	f^2

4) Se observă pe tabla de la pct. 3) că elementul neutru pentru operația indusă pe H este f^3. În raport cu operația indusă simetricul lui f^2 este f^4, al lui f^3 este f^3 și al lui f^4 este f^2.

R – 2 1) Fie A, $B \in M_2(\mathbf{R})$, $A = \begin{pmatrix} a & 0 \\ c & a+d \end{pmatrix}$, $B = \begin{pmatrix} b & 0 \\ c & b+d \end{pmatrix}$.

Verificați că $AB = BA$.

2) Dacă M este o mulțime înzestrată cu o lege de compoziție $M \times M \to M$, $(x, y) \to xy$ asociativă și cu element neutru iar elementele a, $b \in M$ au proprietatea $ab = ba$, atunci

$$a^m b^n = b^n a^m, \qquad \forall m, n \in \mathbf{N}.$$

Soluție. 1) Avem:

$$AB = \begin{pmatrix} a & 0 \\ c & a+d \end{pmatrix}\begin{pmatrix} b & 0 \\ c & b+d \end{pmatrix} = \begin{pmatrix} ab & 0 \\ c(a+b+d) & (a+d)(b+d) \end{pmatrix}$$

și

$$BA = \begin{pmatrix} b & 0 \\ c & b+d \end{pmatrix}\begin{pmatrix} a & 0 \\ c & a+d \end{pmatrix} = \begin{pmatrix} ba & 0 \\ c(a+b+d) & (b+d)(a+d) \end{pmatrix}$$

de unde $AB = BA$.

2) Arătăm mai întîi că $a^m b = ba^m$ oricare ar fi $m \in \mathbf{N}$. Dacă $m = 0$, atunci:

$$a^0 b = eb = be = ba^0.$$

Presupunem că $m > 0$ și că $a^{m-1}b = ba^{m-1}$. Atunci

$$a^m b = (a^{m-1}a)b = a^{m-1}(ab) = a^{m-1}(ba) = (a^{m-1}b)a = (ba^{m-1})a = b(a^{m-1}a) = ba^m$$

și afirmația este demonstrată prin inducție asupra lui m.

Fixăm acum pe m și demonstrăm prin inducție asupra lui n că

$$a^m b^n = b^n a^m, \qquad \forall n \in \mathbf{N}.$$

Dacă $n = 0$ atunci $a^m b^0 = a^m e = ea^m = b^0 a^m$.

Presupunem că $n > 0$ și că $a^m b^{n-1} = b^{n-1}a^m$. Atunci

$$a^m b^n = a^m(b^{n-1}b) = (a^m b^{n-1})b = (b^{n-1}a^m)b = b^{n-1}(a^m b) = b^{n-1}(ba^m) =$$
$$= (b^{n-1}b)a^m = b^n a^m.$$

Exerciții

1. Să se alcătuiască tablele operațiilor induse pe $\mathcal{A}_4 = \{0, 1, 2, 3\} \subset \mathbf{Z}$ de adunarea și înmulțirea modulo 4.

2. Arătați că mulțimea $H = \{0, 1, 2, 3, 4\} \subset \mathbf{Z}$ este stabilă față de legea de compoziție $\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$, $(x, y) \to |x - y|$ și să se alcătuiască tabla operației induse.

3. Arătați că orice submulțime $H \neq \varnothing$ a lui $\mathbf{R}$ este stabilă în raport cu fiecare din legile de compoziție

$$\alpha \perp \beta \overset{\text{def}}{=} \max\{\alpha, \beta\}; \quad \alpha \top \beta \overset{\text{def}}{=} \min\{\alpha, \beta\}, \qquad \forall \alpha, \beta \in \mathbf{R}.$$

Alcătuiți tablele operațiilor induse pe $H = \{\alpha, \beta, \gamma\}$, unde

$$\alpha = \sqrt{5}, \quad \beta = \sqrt{1 + \sqrt{2}}, \quad \gamma = \sqrt[3]{3 + \sqrt{2}}.$$

4. Fie $H = \{a \in \mathbf{N} \mid a \mid 12\}$. Arătați că H este o parte stabilă a lui $\mathbf{N}$ în raport cu fiecare din legile de compoziție:

$$a \perp b \overset{\text{def}}{=} \text{c.m.m.d.c. } \{a, b\}, \quad a \top b \overset{\text{def}}{=} \text{c.m.m.m.c. } \{a, b\}, \quad \forall a, b \in \mathbf{N}.$$

Alcătuiți tablele operațiilor induse.

5. Pentru ce valori ale parametrului real λ intervalul $(2, \infty)$ este o parte stabilă a lui $\mathbf{R}$ în raport cu legea de compoziție

$$x * y \overset{\text{def}}{=} xy - 2x - 2y + \lambda, \quad \forall x, y \in \mathbf{R}.$$

6. Fie $E = \mathbf{R} \setminus \{1/\sqrt{3}, -1/\sqrt{3}\}$ și $f_i : E \to E$, $1 \leqslant i \leqslant 3$ definite astfel:

$$f_1(x) = x, \quad f_2(x) = (x + \sqrt{3})/(1 - x\sqrt{3}), \quad f_3(x) = (x - \sqrt{3})/(1 + x\sqrt{3}), \quad \forall x \in E.$$

Arătați că $H = \{f_1, f_2, f_3\}$ este stabilă în raport cu operația de compunere a funcțiilor și alcătuiți tabla operației induse.

7. Pe $\mathbf{R}$ definim legea de compoziție $\mathbf{R} \times \mathbf{R} \to \mathbf{R}$, $(x, y) \to x * y$, unde $x * y \overset{\text{def}}{=} x + y + xy$. Arătați că această lege de compoziție este asociativă, comutativă și cu element neutru. Intervalul $[-1, \infty)$ este o parte stabilă a lui $\mathbf{R}$ în raport cu legea de compoziție „$*$".

8. Arătați că legile de compoziție de la ex. 3. sînt asociative și comutative. Studiați existența elementului neutru pentru operațiile induse pe intervalele $[a, b]$, $[a, b)$, $(a, b]$, (a, b) unde $a, b \in \mathbf{R}$, $a < b$.

9. Arătați că legile de compoziție definite pe $\mathbf{N}$ la ex. 4 sînt asociative și comutative. Studiați existența elementului neutru pentru aceste legi de compoziție și pentru operațiile induse pe $H = \{a \in \mathbf{N} \mid a \mid 12\}$.

10. Fie $M = \mathbf{N} \times \mathbf{N}$. Pe mulțimea M introducem legile de compoziție:

$$(x, y) + (z, w) \overset{\text{def}}{=} (x + z, y + w),$$

$$(x, y)\ (z, w) \overset{\text{def}}{=} (xz + yw,\ xw + yz)$$

oricare ar fi perechile (x, y) și (z, w) din M. Arătați că aceste legi de compoziție sînt asociative, comutative și cu element neutru.

11. Fie $M = \mathbf{Z} \times \mathbf{Z}^*$, unde $\mathbf{Z}^* = \mathbf{Z} \setminus \{0\}$. Pe mulțimea M introducem următoarele legi de compoziție:

$$(x, y) + (z, w) \overset{\text{def}}{=} (xw + yz,\ yw),$$

$$(x, y)\ (z, w) \overset{\text{def}}{=} (xz,\ yw)$$

oricare ar fi perechile (x, y) și (z, w) din M. Arătați că aceste legi de compoziție sînt asociative, comutative și cu element neutru.

12. Fie $a, b, c \in \mathbf{Z}$, $b \neq 0$. Pe $\mathbf{Z}$ definim legea de compoziție „$*$“,

$$x * y \overset{\text{def}}{=} axy + b(x + y) + c, \qquad \forall x, y \in \mathbf{Z}.$$

1) Arătați că „$*$“ este lege de compoziție asociativă dacă și numai dacă

$$b^2 - b - ac = 0.$$

2) Cînd $b^2 - b - ac = 0$ legea de compoziție „$*$“ are element neutru dacă și numai dacă $b \mid c$.

13. Pe mulțimea $\mathbf{N}$ a numerelor naturale definim legea de compoziție „$*$“

$$\mathbf{N} \times \mathbf{N} \to \mathbf{N}, \qquad (m, n) \to m * n \overset{\text{def}}{=} m^n.$$

1) Cercetați proprietățile acestei legi de compoziție.

2) Determinați tripletele (m, n, p) de numere naturale diferite de 0 astfel încît

$$(m * n) * p = m * (n * p).$$

14. Pe $\mathbf{R}$ se definește legea de compoziție „$*$“

$$\mathbf{R} \times \mathbf{R} \to \mathbf{R}, \quad (x, y) \to x * y \overset{\text{def}}{=} xy + 2ax + by.$$

Determinați a și b astfel încît legea de compoziție „$*$“ să fie comutativă și asociativă.

15. Pe $\mathbf{R}$ se definește legea de compoziție „$*$“,

$$\mathbf{R} \times \mathbf{R} \to \mathbf{R}, \qquad (x, y) \to x * y \overset{\text{def}}{=} xy - x - y - 2.$$

Cercetați existența elementului neutru.

16. Fie M mulțimea matricelor $A \in M_2(\mathbf{R})$,

$$A = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}, \qquad a, b \in \mathbf{R}.$$

Arătați:

1) $A, B \in M \Rightarrow AB \in M$;

2) Nu există $U \in M$ astfel încît $UA = A$, $\forall A \in M$;

3) Există o infinitate de matrice $V \in M$ astfel încît $AV = A$, $\forall A \in M$.

Admite element neutru operația indusă pe M de înmulțiera matricelor?

17. Pe $\mathbf{R}_+^* = \{a \in \mathbf{R} \mid a > 0\}$ definim legile de compoziție:

$$a \perp b \overset{\text{def}}{=} \frac{a + b}{2} \qquad \text{(media aritmetică)}$$

$$a \top b \overset{\text{def}}{=} \sqrt{ab} \qquad \text{(media geometrică)}$$

$$a \,\Delta\, b \overset{\text{def}}{=} \frac{2ab}{a + b} \qquad \text{(media armonică)}$$

$\forall a, b \in \mathbf{R}_+^*$.

Arătați că aceste legi de compoziție sînt comutative și nu sînt asociative. Admit element neutru?

18. Pe $M_2(\mathbf{R})$ se definește legea de compoziție „$*$“,

$$A * B \overset{\text{def}}{=} AB + BA, \qquad \forall A, B \in M_2(\mathbf{R})$$

Studiați dacă legea de compoziție „$*$“ este asociativă (comutativă). Admite element neutru?

19. Determinați părțile stabile finite ale lui $\mathbf{Z}$ în raport cu înmulțirea. Este $\mathbf{R} \setminus \mathbf{Q}$ parte stabilă a lui $\mathbf{R}$ în raport cu adunarea (înmulțirea)?

20. Fie H mulțimea numerelor reale de forma $a + b\sqrt{2}$, $a, b, \in \mathbf{Q}$ ce satisfac condiția $a^2 - 2b^2 = 1$. Arătați că H este o parte stabilă a lui $\mathbf{R}$ în raport cu înmulțirea și că toate numerele din H sînt simetrizabile în raport cu operația indusă.

21. Fie M mulțimea matricelor $A \in M_2(\mathbf{R})$,

$$A = \begin{pmatrix} a & 0 \\ c & b \end{pmatrix}, \qquad a, b, c \in \mathbf{R}.$$

1) Dacă $A, B \in M$, atunci $AB \in M$.

2) Care sînt elementele simetrizabile ale lui M în raport cu operația indusă?

22. Determinați elementele simetrizabile în raport cu înmulțirea modulo 12 din $\mathfrak{R}_{12}$.

23. Examinînd tabla înmulțirii modulo 8, deduceți că pentru ecuația $a * x \oplus b = 0$, cu $a, b \in \mathfrak{R}_8$, $a \neq 0$, sînt posibile numai cazurile:

1) nu are nici o soluție în $\mathfrak{R}_8$;

2) are o singură soluție în $\mathfrak{R}_8$;

3) are două soluții în $\mathfrak{R}_8$;

4) are patru soluții în $\mathfrak{R}_8$.

Dați cîte un exemplu de astfel de ecuație pentru fiecare tip.

24. Găsiți toate soluțiile din $\mathfrak{R}_{12}$ ale sistemului de ecuații liniare

$$3 * x \oplus 4 * y = 11,$$
$$4 * x \oplus 9 * y = 10$$

* * *

25*. Fie $n > 0$ un număr întreg și

$$M = \{(a, b) \mid a, b \in \mathbf{Z},\ (a, n) = 1\}.$$

1) Dacă $(a, b), (c, d) \in M \Rightarrow (ac,\ ad + bc) \in M$;

2) Legea de compoziție „$*$“ definită pe M prin:

$$(a, b) * (c, d) = (ac,\ ad + bc)$$

este comutativă și asociativă.

3) Determinați elementul neutru și elementele simetrizabile.

26*. Pe o mulțime M se dă o lege de compoziție asociativă

$$M \times M \to M, \ (x, y) \to xy$$

cu proprietatea: $\exists a \in M$ astfel încît $\forall y \in M$ avem $y = axa$ cu $x \in M$. Arătați că o asemenea lege de compoziție admite element neutru.

27*. Fie „$\top$" și „$\perp$" două legi de compoziție pe mulțimea M, cu elemente neutre e, respectiv e'. Dacă oricare ar fi $x, y, u, v \in M$ avem:

$$(x \top y) \perp (u \top v) = (x \perp u) \top (y \perp v),$$

atunci:

1) $e = e'$

2) $x \top y = x \perp y, \qquad \forall x, y \in M.$

3) $x \perp y = y \perp x, \qquad \forall x, y \in M.$

28*. Fie M o mulțime cu trei elemente.

1) Cîte legi de compoziție se pot defini pe M?

2) Cîte dintre acestea sînt comutative?

3) Cîte admit element neutru?

Generalizare.

29*. Pe mulțimea punctelor unui plan Π definim legea de compoziție $\varphi : \Pi \times \Pi \to \Pi$, $\varphi(A, B) = C \overset{\text{def}}{\Leftrightarrow} C$ este simetricul lui A în raport cu B.

1) Arătați că φ nu este asociativă și nici comutativă.

2) Raportînd punctele planului la un reper $x_1 0 x_2$, arătați că mulțimea H a punctelor planului de coordonate întregi este inclusă în orice parte stabilă T a lui Π în raport cu φ ce conține punctele de coordonate (0, 0), (1, 0), (0, 1), (1, 1).

30*. Fie M mulțimea tuturor secvențelor de opt litere din alfabetul latin, numite *cuvinte* de lungime 8 peste alfabetul latin. Dacă $\alpha, \beta \in M$, definim cuvintele $\alpha * \beta$ și $\alpha \circ \beta$ astfel: $\alpha * \beta$ este cuvîntul format cu primele 5 litere ale lui α urmate de ultimele trei litere ale lui β iar $\alpha \circ \beta$ este cuvîntul format din ultimele 4 litere ale lui α urmate de primele patru litere ale lui β. Astfel, dacă α = aartbbcd și β = csttrabb, atunci $\alpha * (\beta * \beta)$ = aartbabb și $\alpha \circ \beta$ = bbcdcstt. Arătați că legea de compoziție „$*$" este asociativă iar „$\circ$" nu este asociativă. Studiați comutativitatea.

Capitolul III — GRUPURI

§ 1. METODA AXIOMATICĂ ÎN ALGEBRĂ

Ceea ce deosebește *algebra modernă (abstractă)* de *algebra clasică* este folosirea consecventă a metodei axiomatice. Mai mult sau mai puțin sistematic, această metodă s-a folosit în studiul geometriei euclidiene încă din clasele gimnaziale.

Aplicarea metodei axiomatice în unul sau altul din domeniile matematicii înseamnă:

a) *abstractizare* — ignorarea sistematică a unor aspecte ale obiectelor investigate, declarate neesențiale, și enumerarea exhaustivă a listei de proprietăți *(axiome)* pe care le admitem referitor la obiectele studiate;

b) *interdicția* strictă de a face apel la alte lucruri în afară de axiome și proprietăți ce au fost deja obținute din acestea cu ajutorul regulilor logicii.

Aplicarea metodei axiomatice în algebră are la bază noțiunea de *structură algebrică*: mulțime echipată cu una sau mai multe legi de compoziție ce satisfac o listă specifică de axiome date sub formă de identități sau alte condiții. În acest manual vom studia structurile de *monoid*, *grup*, *inel*, *corp* și de *spațiu vectorial*.

În unele domenii ale matematicii, aplicarea metodei axiomatice are ca rezultat faptul că există, în mod esențial, un singur model ce satisface sistemul de axiome (axiomatica lui Euclid-Hilbert pentru geometria euclidiană, axiomatica lui Peano pentru numerele naturale). Specific pentru structurile algebrice este numărul mare de modele (exemple) pe care le admit, practic nefiind complet cunoscută aria lor de aplicabilitate. Această trăsătură a structurilor algebrice decurge din faptul că în definirea lor se dă statut de axiome la proprietăți ce au fost „semnalate" în multe cazuri „concrete".

Modelele (exemplele) unei structuri algebrice prezintă adesea un interes de-sine-stătător în matematică (grupul permutărilor, grupul deplasărilor, inelul polinoamelor, inelul matricelor, spațiul vectorial $\mathbf{R}^n$ etc.). Rezultatele obținute pentru o structură algebrică dată se transferă printr-o simplă traducere la orice model al structurii, ceea ce reprezintă unul din principalele avantaje ale folosirii metodei axiomatice în algebră. Totodată se pune într-o lumină nouă modelul structurii, obținîndu-se rezultate care ar fi fost greu de descifrat în desișul de detalii ale acestuia.

În fine, să menționăm faptul că, într-o clasificare dată de unii autori, calculul în matematică poate să fie:

1) *calcul aproximativ* (care obține și prelucrează inegalități, fiind obiectul Analizei).

2) *calcul algebric* (care obține și prelucrează identități, fiind obiectul Algebrei).

În legătură cu această clasificare, se cuvine să observăm că metoda axiomatică permite o sistematizare a calculului algebric și adesea renunțarea la acesta, în favoarea raționamentului conceptual.

§ 2. MONOIZI

Așa cum s-a menționat în § 1, algebra modernă are ca obiect studiul structurilor algebrice. Prin *structură algebrică* se înțelege o mulțime nevidă M înzestrată cu una sau mai multe legi de compoziție φ, ψ, ..., ce satisfac o listă specifică de proprietăți, numite *axiomele* structurii.

Prima structură algebrică pe care o introducem este structura de monoid. Prin *monoid* se înțelege un cuplu (M, φ) format cu o mulțime nevidă M și o lege de compoziție definită pe M, $\varphi : M \times M \to M$, asociativă și cu element neutru. Se mai spune că M este (formează) monoid în raport cu operația φ.

Mai sistematic, folosind de exemplu notația „$*$" pentru legea de compoziție, definiția monoidului se poate da astfel:

2.1. *Definiție.* **O mulțime nevidă M este monoid în raport cu o lege de compoziție definită pe M,**

$$M \times M \to M, \quad (x, y) \to x * y$$

dacă sînt satisfăcute următoarele axiome:

M_1) $\quad (x * y) * z = x * (y * z), \qquad \forall x, y, z \in M;$

M_2) $\exists e \in M$ **astfel încît** $e * x = x * e = x, \ \forall x \in M.$

Dacă pentru legea de compoziție φ a monoidului se folosește una din notațiile „$*$", „$+$", „ $\cdot$" etc. atunci în loc de (M, φ) scriem $(M, *)$, $(M, +)$, $(M, .)$ etc.

Adesea cuplul (M, φ) se notează tot cu M; în acest caz M se interpretează fie ca fiind cuplul (M, φ), fie ca fiind mulțimea *suport (subiacentă)* a structurii de monoid.

Ansamblul de condiții M_1, M_2 poartă numele de *axiomele monoidului.* Elementul $e \in M$ care satisface axioma M_2 este unic determinat (v. Teorema 6.2, Cap. II) și se numește *elementul neutru* al monoidului M.

Vom nota cu $U(M)$ mulțimea elementelor lui M simetrizabile în raport cu operația acestuia. Cînd M este dat în notație multiplicativă, elementele din $U(M)$ se mai numesc încă și *unități* ale monoidului M.

Spunem că monoidul M este *comutativ* dacă operația acestuia satisface și axioma:

M_3) $\qquad x * y = y * x, \qquad \forall x, y \in M.$

Exemple

1. Adunarea numerelor este asociativă, comutativă și admite pe 0 ca element neutru. Rezultă că $(\mathbb{N}, +)$ este monoid comutativ, numit *monoidul aditiv* al numerelor naturale. De asemenea, $(\mathbb{N}, \cdot)$ este monoid comutativ, numit *monoidul multiplicativ* al numerelor naturale.
2. Fie E o mulțime și $\mathfrak{P}(E)$ mulțimea tuturor părților lui E.

   Cum:

   M_1) $\quad (X \cup Y) \cup Z = X \cup (Y \cup Z), \qquad \forall X, Y, Z \in \mathfrak{P}(E)$

   M_2) $\quad \varnothing \cup X = X \cup \varnothing = X, \qquad \forall X \in \mathfrak{P}(E)$

   M_3) $\quad X \cup Y = Y \cup X, \qquad \forall X, Y, Z \in \mathfrak{P}(E)$

   rezultă că $(\mathfrak{P}(E), \cup)$ este monoid comutativ.

   Analog, $(\mathfrak{P}(E), \cap)$ este monoid comutativ.
3. Fie E o mulțime și $\mathfrak{F}(E)$ mulțimea tuturor funcțiilor $f : E \to E$. Cum:

   M_1) $\quad (f \circ g) \circ h = f \circ (g \circ h), \qquad \forall f, g, h \in \mathfrak{F}(E)$

   M_2) $\quad 1_E \circ g = f \circ 1_E = f, \qquad \forall f \in \mathfrak{F}(E)$

   rezultă că $\mathfrak{F}(E)$ formează monoid în raport cu operația de compunere. Dacă E are cel puțin două elemente, atunci $(\mathfrak{F}(E), \circ)$ nu este monoid comutativ (v. tabla operației lui $\mathfrak{F}(E)$ cînd $E = \{1, 2\}$; Cap. II, § 3).

   Să observăm că într-un monoid M calculul algebric are proprietățile date în § 9, Cap. II, și totodată sînt adevărate toate rezultatele obținute în Cap. II în legătură cu elementele simetrizabile.

Exerciții rezolvate

R—1 Fie M mulțimea tuturor matricelor $A \in M_2(\mathbb{Z})$ de forma:

$$A = \begin{pmatrix} a & c \\ 0 & b \end{pmatrix}, \quad a, b, c \in \mathbb{Z}.$$

1) Să se arate că M este o parte stabilă a lui $M_2(\mathbb{Z})$ în raport cu înmulțirea matricelor și că formează monoid în raport cu operația indusă;

2) Determinați elementele simetrizabile ale monoidului M.

Soluție. 1) Fie $A, B \in M_2(\mathbb{Z})$,

$$A = \begin{pmatrix} a & c \\ 0 & b \end{pmatrix}, \quad B = \begin{pmatrix} u & w \\ 0 & v \end{pmatrix}.$$

Avem:

$$AB = \begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \begin{pmatrix} u & w \\ 0 & v \end{pmatrix} = \begin{pmatrix} au & aw + cv \\ 0 & bv \end{pmatrix} \in M.$$

Rezultă că M este o parte stabilă a lui $M_2(\mathbb{Z})$ în raport cu înmulțirea matricelor.

Cum

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M$$

rezultă că operația indusă pe M admite element neutru, anume pe E. Operația indusă este și asociativă căci înmulțirea matricelor este asociativă. Rezultă că $(M,.)$ este monoid.

2) Presupunem că $A \in U(M)$. Atunci există $B \in M_2(\mathbf{Z})$ astfel încît $AB = BA = E$. Cum

$$1 = \det(E) = \det(AB) = \det(A)\det(B)$$

și $\det(A)$, $\det(B)$ sînt numere întregi, rezultă că $\det(A) = \pm 1$, deci

$$ab = \begin{vmatrix} a & c \\ 0 & b \end{vmatrix} = \pm 1.$$

Cum $a, b \in \mathbf{Z}$ rezultă că $ab = 1$ dacă $a = 1$, $b = 1$ sau $a = -1$, $b = -1$, și $ab = -1$ dacă $a = -1$, $b = 1$ sau $a = 1$, $b = -1$. Așadar, dacă $A \in U(M)$ atunci A este egală cu una din matricele:

$$\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & c \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1 & c \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & c \\ 0 & -1 \end{pmatrix}, \quad c \in \mathbf{Z}.$$

Reciproc, matricele din lista precedentă sînt elemente inversabile ale monoidului M, inversele lor fiind respectiv matricele:

$$\begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & -c \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1 & c \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & c \\ 0 & -1 \end{pmatrix}, \quad c \in \mathbf{Z}$$

după cum ușor se poate verifica.

R—2 Fie E o mulțime nevidă și $f \in \mathfrak{F}(E)$. Următoarele afirmații sînt echivalente:

a) f este element simetrizabil al monoidului $(\mathfrak{F}(E), \circ)$;

b) f este funcție bijectivă.

Enumerați elementele simetrizabile ale monoidului $(\mathfrak{F}(E), \circ)$, unde $E = \{1, 2, 3\}$.

Soluție. a) $\Rightarrow$ b). Cum f este element simetrizabil, există $g \in \mathfrak{F}(E)$ astfel încît:

$$f \circ g = g \circ f = 1_E.$$

Rezultă că f este funcție bijectivă (v. Ex. **R-3,** Cap. I).

b) $\Rightarrow$ a). Cum $f : E \to E$ este funcție bijectivă, pentru orice $y \in E$ există $x \in E$ unic determinat astfel încît $y = f(x)$. Definim $g : E \to E$ prin:

$$g(y) \overset{\text{def}}{=} x \Leftrightarrow f(x) = y, \quad \forall y \in E.$$

Avem:

$$(f \circ g)(y) = f(g(y)) = f(x) = y = 1_E(y), \quad \forall y \in E$$

și

$$(g \circ f)(x) = g(f(x)) = g(y) = x = 1_E(x), \quad \forall x \in E,$$

de unde

$$f \circ g = g \circ f = 1_E$$

deci f este element simetrizabil al monoidului $(\mathfrak{F}(E), \circ)$.

Presupunem că $E = \{1, 2, 3\}$ și $f \in \mathfrak{F}(E)$. Cu convenția de la § 3, cap. II, funcția f se poate da prin:

$$f = \begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}.$$

Evident, $\mathfrak{F}(E)$ are $3 \times 3 \times 3 = 27$ elemente, f fiind simetrizabil (= bijectiv) dacă și numai dacă valorile sale $f(1)$, $f(2)$, $f(3)$ reproduc, într-o ordine arbitrară, numerele 1, 2, 3. Avem deci $3! = 6$ elemente simetrizabile, anume:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Așadar $U(\mathfrak{F}(E)) = \{e, \sigma, \pi, \alpha, \beta, \gamma\}$.

§ 3. DEFINIȚIA GRUPULUI. EXEMPLE

Noțiunea de grup ocupă un loc central printre structurile algebrice. Teoria grupurilor are în esență o sursă unică: *studiul, în raport cu operația de compunere, al funcțiilor bijective ale unei mulțimi în ea însăși.*

Definiția noțiunii de *grup* se dă imediat cu ajutorul celei de monoid: un monoid G cu proprietatea că orice element $x \in G$ este simetrizabil (în raport cu operația acestuia) se numește *grup*. Mai precis:

3.1. *Definiție.* **Un cuplu $(G, *)$ format cu o mulțime nevidă G și cu o lege de compoziție pe G,**

$$G \times G \to G, \qquad (x, y) \to x * y$$

se numește *grup* dacă sînt satisfăcute următoarele axiome:

G_1) $(x * y) * y = x * (y * z), \quad \forall x, y, z \in G;$

G_2) $\exists e \in G$ **astfel încît** $e * x = x * e = x, \quad \forall x \in G;$

G_3) $\forall x \in G, \quad \exists x' \in G$ **astfel încît** $x' * x = x * x' = e.$

Elementul $e \in G$, a cărui existență este asigurată de axioma G_2) este unic determinat (v. Teorema 6.2, Cap. II) și se numește *elementul neutru* al grupului G. Elementul x' a cărui existență este asigurată de axioma G_3) pentru orice $x \in G$, este unic determinat (v. § 7, Cap. II) și se numește *simetricul* lui x; în notația multiplicativă punem $x' = x^{-1}$, iar în notația aditivă punem $x' = -x$, numit *inversul*, respectiv *opusul* lui x.

Ansamblul de condiții G_1), G_2) și G_3) poartă numele de *axiomele grupului.* Dacă în plus este satisfăcută și axioma:

G_4) $x * y = y * x, \quad \forall x, y \in G,$

atunci G se numește grup *comutativ* sau *abelian.*

Exemple

1. *Grupul permutărilor.* Fie $E = \{1, 2, 3\}$.

Să notăm cu $\mathfrak{S}_3$ mulțimea tuturor funcțiilor bijective de la E la E. Folosind convenția de la § 3, cap. II, acestea pot fi descrise astfel:

$$1_E = e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

deci $\mathfrak{S}_3 = \{e, \sigma, \pi, \alpha, \beta, \gamma\}$.

Cum compusa a două funcții bijective este o funcție bijectivă (v. Teorema 3.1. Cap. 1) rezultă că $\mathfrak{S}_3$ este o parte stabilă a lui $\mathfrak{F}(E)$ în raport cu compunerea funcțiilor.

Să alcătuim tabla operației induse pe $\mathfrak{S}_3$ de către compunerea funcțiilor, operație numită *compunerea permutărilor* de trei obiecte.

$\circ$	e	σ	π	α	β	γ
e	e	σ	π	α	β	γ
σ	σ	π	e	γ	α	β
π	π	e	σ	β	γ	α
α	α	β	γ	e	σ	π
β	β	γ	α	π	e	σ
γ	γ	α	β	σ	π	e

Tabla grupului $\mathfrak{S}_3$

Avem, de exemplu, $\sigma \circ \alpha = \gamma$. În adevăr,

$$(\sigma \circ \alpha)(1) = \sigma(\alpha(1)) = \sigma(1) = 2 = \gamma(1),$$

$$(\sigma \circ \alpha)(2) = \sigma(\alpha(2)) = \sigma(3) = 1 = \gamma(2),$$

$$(\sigma \circ \alpha)(3) = \sigma(\alpha 3)) = \sigma(2) = 3 = \gamma(3)$$

de unde $\sigma \circ \alpha = \gamma$.

Cum compunerea funcțiilor este asociativă și $1_E = e \in \mathfrak{S}_3$, rezultă că $(\mathfrak{S}_3, \circ)$ este monoid. Se observă pe tabla operației lui $\mathfrak{S}_3$ că orice element din $\mathfrak{S}_3$ este simetrizabil, anume:

$$e^{-1} = e, \ \sigma^{-1} = \pi, \ \pi^{-1} = \sigma, \ \alpha^{-1} = \alpha, \ \beta^{-1} = \beta, \ \gamma^{-1} = \gamma.$$

Rezultă că $(\mathfrak{S}_3, \circ)$ este grup, numit *grupul permutărilor* de trei obiecte sau încă *grupul simetric* de grad 3. Din tabla operației lui $\mathfrak{S}_3$ rezultă că acesta nu este grup comutativ.

Analog, dacă $n > 1$ și $E = \{1, 2, \ldots, n\}$ atunci mulțimea $\mathfrak{S}_n$ a funcțiilor bijective de la E la E formează grup în raport cu operația de compunere a funcțiilor; $(\mathfrak{S}_n, \circ)$ se numește *grupul permutărilor* de n obiecte sau *grupul simetric* de grad n.

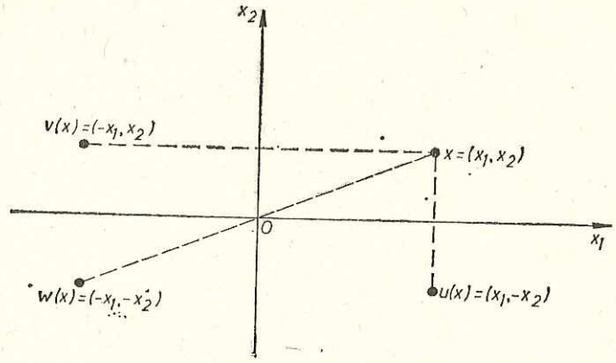


Fig. III.1

2. *Grupul lui Klein.* Fie $E = \mathbf{R} \times \mathbf{R}$ și $\mathfrak{K} = \{1_E, u, v, w\}$, unde u, v și w sînt următoarele funcții de la E la E (v. fig. III.1);

$$u : E \to E, \quad u(x) = (x_1, -x_2),$$

$$v : E \to E, \quad v(x) = (-x_1, x_2),$$

$$w : E \to E, \quad w(x) = (-x_1, -x_2),$$

oricare ar fi $x = (x_1, x_2) \in E = \mathbf{R} \times \mathbf{R}$.

Dacă compunem două funcții din $\mathfrak{K}$ se obține tot o funcție din $\mathfrak{K}$. De exemplu, avem $u \circ v = w$. În adevăr, pentru orice $x \in E$, $x = (x_1, x_2)$, avem:

$$(u \circ v)(x) = u(v(x)) = u((-x_1, x_2)) = (-x_1, -x_2) = w(x),$$

de unde $u \circ v = w$. Să alcătuim tabla operației indusă pe $\mathfrak{K}$ de către compunerea funcțiilor din $\mathfrak{F}(E)$.

$\circ$	1_E	u	v	w
1_E	1_E	u	v	w
u	u	1_E	w	v
v	v	w	1_E	u
w	w	v	u	1_E

Tabla grupului Klein

Cum compunerea funcțiilor este asociativă și $1_E \in \mathfrak{K}$, rezultă că $(\mathfrak{K}, \circ)$ este monoid. Se observă pe tabla operației lui $\mathfrak{K}$ că orice element din $\mathfrak{K}$ este simetrizabil, anume:

$$1_E^{-1} = 1_E, \ u^{-1} = u, \ v^{-1} = v, \ w^{-1} = w.$$

Așadar $(\mathfrak{K}, \circ)$ este grup, numit grupul lui Klein. Din tabla operației, se deduce că grupul lui Klein este comutativ. Să observăm că elementele grupului $\mathfrak{K}$ sînt funcții bijective. Aceasta se poate verifica direct sau ob-

servind că $u \circ u = 1_E$, $v \circ v = 1_E$, $w \circ w = 1_E$ și aplicînd apoi rezultatul de la Ex. R-3, Cap. I.

3. *Grupul* $(\mathcal{R}_n, \oplus)$ *al resturilor modulo* n. Fie $n = 4$ și $\mathcal{R}_4 = \{0, 1, 2, 3\}$. Se știe că $\mathcal{R}_4$ este o parte stabilă a lui $\mathbf{Z}$ în raport cu adunarea modulo 4. Să alcătuim tabla operației induse.

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Tabla grupului $(\mathcal{R}_4, \oplus)$

Operația indusă pe $\mathcal{R}_4$ de către adunarea modulo 4 este asociativă (v. § 8, Cap. II). Din tabla acestei operații rezultă că admite pe 0 ca element neutru, că este comutativ și că orice element din $\mathcal{R}_4$ este simetrizabil în raport cu operația indusă:

$$-0 = 0, \quad -1 = 3, \quad -2 = 2, \quad -3 = 1$$

Așadar, $(\mathcal{R}_4, \oplus)$ este grup abelian. Analog se arată că $(\mathcal{R}_n, \oplus)$ este grup abelian, unde $\mathcal{R}_n = \{0, 1, 2, \ldots, n-1\}$ iar „$\oplus$" este operația indusă pe $\mathcal{R}_n$ de către adunarea modulo n, numit *grupul resturilor modulo n.*

4. Din proprietățile adunării și înmulțirii numerelor, menționate în Cap. I, § 1, rezultă că

$$(\mathbf{Z}, +), \ (\mathbf{Q}, +), \ (\mathbf{R}, +) \text{ și } (\mathbf{C}, +)$$

sînt grupuri abeliene, numite respectiv *grupul aditiv* al numerelor întregi, raționale, reale, complexe.

De asemenea, notînd

$$\mathbf{Q}^* = \mathbf{Q} \setminus \{0\}, \ \mathbf{R}^* = \mathbf{R} \setminus \{0\} \text{ și } \mathbf{C}^* = \mathbf{C} \setminus \{0\},$$

atunci

$$(\mathbf{Q}^*, \cdot), \ (\mathbf{R}^*, \cdot) \text{ și } (\mathbf{C}^*, \cdot)$$

sînt grupuri *abeliene*, numite respectiv *grupul multiplicativ* al numerelor raționale, reale complexe diferite de zero.

§ 4. REGULI DE CALCUL ÎNTR-UN GRUP

Cum orice grup este monoid, calculul algebric cu elementele unui grup beneficiază de toate regulile valabile pentru legile de compoziție asociative și cu element neutru.

Pe de altă parte, pentru grupuri avem o serie de reguli care nu sînt întotdeauna aplicabile în cazul monoizilor. În esență, aceste reguli se fundamentează pe proprietatea că orice element al unui grup este simetrizabil în raport cu operația acestuia.

4.1. **Teoremă. Într-un grup** G **sînt adevărate regulile de simplificare la stînga și la dreapta:**

$$\boxed{a * b = a * c \Rightarrow b = c},$$

respectiv

$$\boxed{b * a = c * a \Rightarrow b = c}.$$

Demonstrație. Presupunem că pentru $a, b, c \in G$ avem $a * b = a * c$ și fie a' simetricul elementului a. Avem:

$$b = e * b = (a' * a) * b = a' * (a * b) = a' * (a * c) = (a' * a) * c = e * c = c,$$

deci $b = c$, de unde rezultă că este adevărată regula de simplificare la stînga. Analog se demonstrează regula de simplificare la dreapta.

4.2. **Teoremă. Fie** $(G,*)$ **un grup. Oricare ar fi** $a, b \in G$, **ecuațiile:**

$$a * x = b \quad \text{și} \quad y * a = b$$

au soluții unice în G, **anume** $x = a' * b$, **respectiv** $y = b * a'$, **unde** a' **este simetricul lui** a.

Demonstrație. Dacă x_1 și x_2 sînt soluții din G ale ecuației $a * x = b$, atunci

$$a * x_1 = b = a * x_2,$$

deci $a * x_1 = a * x_2$ și folosind regula de simplificare la stînga obținem $x_1 = x_2$. Așadar, ecuația $a * x = b$ are cel mult o soluție în G.

Fie $x = a' * b$, unde a' este simetricul lui a.
Avem:

$$a * x = a * (a' * b) = (a * a') * b = e * b = b,$$

de unde rezultă că $x = a' * b$ este soluție (din G) a ecuației $a * x = b$, unică conform primei părți a demonstrației. Analog se arată că ecuația $y * a = b$ admite soluție unică, $y = b * a'$.

Dacă grupul G este dat în notația aditivă (multiplicativă) atunci rezultatele din teoremele precedente se transcriu astfel:

$$a + b = a + c \text{ sau } b + a = c + a \Rightarrow b = c,$$
$$a + x = b \Rightarrow x = (-a) + b,$$
$$y + a = b \Rightarrow y = b + (-a) = b - a,$$

respectiv

$$ab = ac \text{ sau } ba = ca \Rightarrow b = c,$$
$$ax = b \Rightarrow x = a^{-1}b,$$
$$ya = b \Rightarrow y = ba^{-1}.$$

Cum operația unui grup este asociativă și cu element neutru, toate rezultatele din §9, Cap. II sînt adevărate și în cazul grupurilor. Astfel, dacă G este grup multiplicativ, $a \in G$ și $n \in \mathbb{N}$, atunci punînd

$$a^n = \begin{cases} e & \text{dacă } n = 0 \\ a^{n-1}\, a & \text{dacă } n > 0 \end{cases}$$

avem:

$$a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn}, \quad \forall\ m,n \in \mathbb{N}.$$

Pentru elementele unui grup putem defini și puteri ale acestora cu exponenți numere întregi negative, după cum urmează.

Dacă $a \in G$ și $n \in \mathbb{Z}$, $n < 0$, atunci $-n > 0$, deci are sens a^{-n} precum și inversul acestuia, anume $(a^{-n})^{-1}$. Punem deci:

$$a^n \overset{\text{def}}{=} (a^{-n})^{-1}, \qquad \forall n \in \mathbb{Z},\ n < 0.$$

și avem:

$$\boxed{a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn}, \quad \forall m,\ n \in \mathbb{Z}}$$

O cale de demonstrație a acestei afirmații este reducerea la cazul exponenților nenegativi, care a fost deja demonstrat (v. § 9, Cap. II).

Astfel, dacă $m < 0$ și $n < 0$ avem:

$$a^m a^n = (a^{-m})^{-1}(a^{-n})^{-1} = (a^{-n} \cdot a^{-m})^{-1} = (a^{(-n)+(-m)})^{-1} = (a^{-(m+n)})^{-1} = a^{m+n}.$$

Presupunem că $m > 0$, $n < 0$. Dacă $|m| \geqslant |n|$ există $r > 0$ astfel încît $m = -n + r$ și atunci

$$a^m a^n = a^{r+(-n)} a^n = a^r a^{-n} (a^{-n})^{-1} = a^r = a^{m+n}$$

ș.a.m.d.

Dacă grupul G este dat în notație aditivă, atunci cele de mai sus devin proprietăți pentru *multiplii întregi* ai elementelor lui G:

$$\boxed{ma + na = (m+n)a, \qquad n(ma) = (nm)a, \qquad \forall m,\ n \in \mathbb{Z}}.$$

Cum pentru orice $a \in G$ și $n \in \mathbb{Z}$ avem

$$a^n a^{-n} = a^{n+(-n)} = a^0 = e = a^{(-n)} a^n$$

rezultă că:

$$\boxed{(a^n)^{-1} = a^{-n}, \quad \forall a \in G, \quad n \in \mathbb{Z}}.$$

Analog, în notație aditivă avem:

$$\boxed{-(na) = (-n)a, \qquad \forall a \in G,\ n \in \mathbb{Z}}.$$

Exerciții rezolvate

R—1 Fie $\varepsilon = -\frac{1}{2} + \frac{i\sqrt{3}}{2} \in \mathbb{C}$. Arătați că

$$\varepsilon^{n^3-n+1} = \varepsilon, \qquad \forall n \in \mathbb{Z}.$$

Soluție. Cum $\varepsilon = \cos\frac{2\pi}{3} + i \sin\frac{2\pi}{3}$, avem:

$$\varepsilon^3 = \cos 2\pi + i \sin 2\pi = 1.$$

Observînd că $n^3 - n = (n-1)n(n+1)$, rezultă că $n^3 - n$ se divide cu 3, deci $n^3 - n = 3q$, cu $q \in \mathbb{Z}$. Dar ε este element al grupului $(\mathbb{C}^*, \cdot)$ și folosind regulile de calcul cu puterile întregi ale unui element dintr-un grup multiplicativ, avem:

$$\varepsilon^{n^3-n+1} = \varepsilon^{3q+1} = \varepsilon^{3q} \cdot \varepsilon^1 = (\varepsilon^3)^q \varepsilon = 1^q \varepsilon = \varepsilon.$$

R—2 Arătați că în orice linie (coloană) a tablei operației unui grup G cu un număr finit de elemente, fiecare element al lui G apare o dată și numai o singură dată.

Soluție. Presupunem că operația grupului G este notată multiplicativ și că $G = \{a_1, a_2, \ldots, a_n\}$, cu $a_i \neq a_j$ pentru $i \neq j$. Fie $a \in G$. În linia lui a din tabla operației grupului G apar elementele:

$$aa_1,\ aa_2,\ \ldots,\ aa_i,\ \ldots,\ aa_n.$$

Dacă $i \neq j$, atunci $aa_i \neq aa_j$. În adevăr, dacă $aa_i = aa_j$, prin simplificare cu a se obține $a_i = a_j$. Contradicție. Rezultă că elementele $aa_1, aa_2, \ldots, aa_n$ sînt distincte și, mai puțin eventual ordinea, coincid cu $a_1, a_2, \ldots, a_n$.

R—3 Fie G un grup multiplicativ cu patru elemente, $G = \{e, a, b, c\}$, unde e este elementul neutru. Alcătuiți tabla operației grupului G dacă se știe că $a^2 = e$ și $c^2 = e$.

Soluție. Cunoscînd că e este element neutru și că $a^2 = c^2 = e$, în tabla operației lui G se pot completa următoarele poziții:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	?	?
b	b	?	?	?
c	c	?	?	e

Ca să nu avem repetiții în linia lui a sau în coloana lui b, la intersecția acestora nu putem pune a, e sau b, deci $ab = c$. Analog se arată apoi succesiv că $ac = b$, $bc = a$, $bb = e$, $ba = c$, $ca = b$, $cb = a$.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

R—4 Fie $(G, \cdot)$ un grup cu n elemente și e elementul neutru al lui G.

1) Demonstrați în cazul cînd G este comutativ că

$$a^n = e, \qquad \forall a \in G.$$

2) Verificați această proprietate în cazul grupului $\mathfrak{S}_3$.

Soluție. 1) Fie $a_1, a_2, \ldots, a_n$ elementele grupului G și fie a un element arbitrar din G. Conform cu Ex. R-2, elementele

$$aa_1, aa_2, \ldots, aa_n$$

coincid, mai puțin eventual ordinea, cu $a_1, a_2, \ldots, a_n$ și cum G este comutativ avem:

$$a_1a_2 \ldots a_n = aa_1 \cdot aa_2 \ldots aa_n = \underbrace{aa \ldots aa}_{n \text{ ori}} a_1a_2 \ldots a_n = a^n a_1a_2 \ldots a_n.$$

Așadar:

$$e(a_1a_2 \ldots a_n) = a^n(a_1a_2 \ldots a_n)$$

și prin simplificare se obține $e = a^n$.

2) Grupul $\mathfrak{S}_3$ are 6 elemente, deci $n = 6$.

Păstrînd notațiile folosite la § 3 pentru elementele grupului $\mathfrak{S}_3$ și folosind tabla operației grupului $\mathfrak{S}_3$ se obține $\sigma^3 = e$, $\pi^3 = e$, $\alpha^2 = e$, $\beta^2 = e$, $\gamma^2 = e$. Astfel din tabla operației grupului $\mathfrak{S}_3$ deducem:

$$\sigma^2 = \sigma \circ \sigma = \pi, \ \sigma^3 = \sigma^2 \circ \sigma = \pi \circ \sigma = e.$$

Avem:

$$\sigma^6 = \sigma^{3\times 2} = (\sigma^3)^2 = e^2 = e, \ \alpha^6 = \alpha^{2\times 3} = (\alpha^2)^3 = e^3 = e \text{ etc.}$$

Observație. Se poate demonstra că rezultatul de la pct. 1) este adevărat și pentru grupuri necomutative, așa cum dealtfel s-a verificat pentru grupul $\mathfrak{S}_3$.

§ 5. SUBGRUP. EXEMPLE

Fizionomia unui grup G se descrie în esență cu ajutorul subgrupurilor sale: submulțimi nevide H ale lui G cărora operația lui G le conferă, de asemenea, o structură de grup.

Mai precis:

5.1. *Definiție.* **Fie $(G, *)$ un grup. O submulțime nevidă H a lui G se numește *subgrup* al lui G dacă sînt satisfăcute următoarele condiții:**

1) $\forall x, y \in H \Rightarrow x * y \in H$;

2) $\forall x \in H \Rightarrow x' \in H$,

unde x' este simetricul lui x (în raport cu operația lui G).

Dacă grupul G este dat în notația aditivă, atunci condițiile 1) și 2) din definiția subgrupului se transcriu astfel:

1) $\forall x, y \in H \Rightarrow x + y \in H$;

2) $\forall x \in H \Rightarrow -x \in H$.

5.2. **Teoremă. Fie $(G, *)$ un grup, e elementul neutru al lui G și H un subgrup al lui G. Atunci:**

1) $e \in H$,

2) **H este grup în raport cu operația indusă pe H de către operația grupului G.**

Demonstrație. 1) Cum $H \neq \varnothing$ putem alege un element $x \in H$. Din 2) rezultă că și $x' \in H$ și acum din 1) rezultă că $e = x' * x \in H$.

2) Să notăm cu φ operația grupului G, $\varphi : G \times G \to G$. Din 1) rezultă că H este o parte stabilă a lui G în raport cu operația φ. Fie φ' legea de compoziție indusă pe H de φ,

$$\varphi' : H \times H \to H, \ (x, y) \to \varphi'(x, y) \overset{\text{def}}{=} \varphi(x, y).$$

Evident φ' este asociativă (căci φ este asociativă) și admite ca element neutru pe $e \in H$. Dacă $x \in H$, atunci simetricul său x' în raport cu φ se găsește în H, deci este simetric al lui x și în raport cu φ'. Rezultă că (H, φ') este grup.

Exemple.

1. Fie $(G, *)$ un grup, e elementul său neutru și $E = \{e\}$. Atunci E este subgrup al lui G, numit *subgrupul unitate*. În adevăr, dacă $x, y \in E$, atunci $x = y = e$, deci

$$x * y = e * e = e \in E,$$
$$x' = e' = e \in E.$$

Dacă G este dat în notație aditivă, atunci $0 = \{0\}$ este subgrup al lui G, numit *subgrupul zero*.

2. Fie $\mathfrak{S}_3$ grupul permutărilor de trei obiecte, $\mathfrak{S}_3 = \{e, \sigma, \pi, \alpha, \beta, \gamma\}$. Următoarele submulțimi ale lui $\mathfrak{S}_3$:

$$E = \{e\}, \ H_1 = \{e, \sigma, \pi\}, \ H_2 = \{e, \alpha\}, \ H_3 = \{e, \beta\}, \ H_4 = \{e, \gamma\}$$

sînt subgrupuri ale lui $\mathfrak{S}_3$. Să facem verificare pentru H_1. Din tabla operației grupului $\mathfrak{S}_3$ se deduce că elementele lui H_1 se compun conform tablei următoare

$\circ$	e	σ	π
e	e	σ	π
σ	σ	π	e
π	π	e	σ

Se observă pe această tablă că H_1 este o parte stabilă a lui $\mathfrak{S}_3$ în raport cu compunerea precum și cu operația de trecere la invers, deci H_1 este subgrup al lui $\mathfrak{S}_3$.

3. Fie $n \geqslant 0$ un număr întreg și $n\mathbb{Z}$ mulțimea tuturor multiplilor lui n,

$$n\mathbb{Z} \overset{\text{def}}{=} \{nh \mid h \in \mathbb{Z}\}.$$

Atunci $n\mathbf{Z}$ este subgrup al grupului $(\mathbf{Z}, +)$. În adevăr, dacă $x, y \in n\mathbf{Z}$, există $h, k \in \mathbf{Z}$ astfel încît $x = nh$, $y = nk$. Rezultă că

$$x + y = nh + nk = n(h + k) \in n\mathbf{Z},$$

$$-x = -(nh) = n(-h) \in n\mathbf{Z},$$

deci $n\mathbf{Z}$ este subgrup al lui $(\mathbf{Z}, +)$.

Exerciții rezolvate

R—1 Fie $H = \{1, i, -1, -i\} \subset \mathbb{C}$. Arătați că H este subgrup al grupului $(\mathbb{C}^*, \cdot)$.

Soluție. Numerele din H se înmulțesc conform tablei următoare:

$\cdot$	1	i	−1	−i
1	1	i	−1	−i
i	i	−1	−i	1
−1	−1	−i	1	i
−i	−i	1	i	−1

Se deduce din tabla înmulțirii elementelor lui H că H este o parte stabilă a lui $\mathbb{C}^*$ în raport cu înmulțirea. În plus, $1^{-1} = 1 \in H$, $i^{-1} = -i \in H$, $(-1)^{-1} = -1 \in H$, $(-i)^{-1} = i \in H$, deci H este subgrup al lui $(\mathbb{C}^*, \cdot)$.

R—2 . Fie $n > 0$, $\zeta = \cos\dfrac{2\pi}{n} + i \sin\dfrac{2\pi}{n}$ și

$$U_n = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}.$$

1) Arătați că U_n este un subgrup cu n elemente al grupului $(\mathbb{C}^*, \cdot)$, numit *grupul rădăcinilor* de ordin n ale unității.

2) Reprezentați geometric elementele lui U_3, U_4, și U_5.

Soluție. 1) Să arătăm că numărul complex ζ are următoarele două proprietăți:

a) $\zeta^n = 1$;

b) $\zeta^h = 1$, $h \in \mathbf{Z} \Rightarrow n \mid h$.

Într-adevăr, folosind formula lui Moivre avem:

$$\zeta^n = \left(\cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}\right)^n = \cos 2\pi + i \sin 2\pi = 1.$$

Fie acum $h \in \mathbf{Z}$ astfel încît $\zeta^h = 1$. Atunci

$$1 = \zeta^h = \cos\frac{2h\pi}{n} + i \sin\frac{2h\pi}{n},$$

deci există $h \in \mathbf{Z}$ astfel încît

$$\frac{2h\pi}{n} = 2\pi h.$$

Rezultă $h = nh$, deci $n \mid h$.

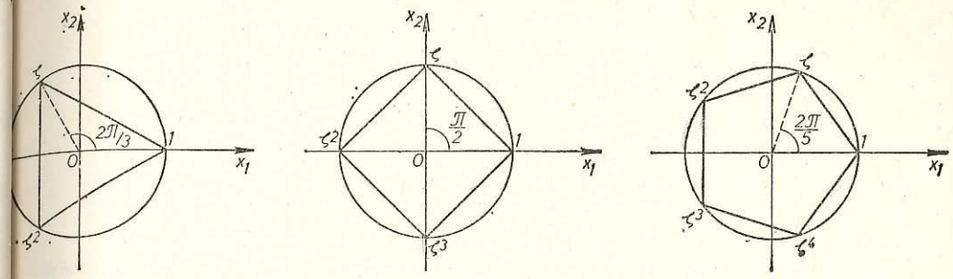


Fig. III.2

Să arătăm că elementele lui U_n sînt distincte, deci că U_n are n elemente. În caz contrar, există $i \neq j$, $0 \leqslant i < j < n$, astfel încît $\zeta^i = \zeta^j$. Înmulțind această egalitate cu ζ^{-i} obținem:

$$1 = \zeta^i \zeta^{-i} = \zeta^j \zeta^{-i} = \zeta^{j-i}$$

și aplicînd b) deducem $n \mid j - i$. Contradicție, căci $0 < j - i < n$.

Fie acum $x, y \in U_n$, $x = \zeta^i$, $y = \zeta^j$, $0 \leqslant i, j < n$. Fie $q, r \in \mathbf{Z}$ astfel încît $i + j = nq + r$, $0 \leqslant r < n$. Avem:

$$xy = \zeta^i \zeta^j = \zeta^{i+j} = \zeta^{nq+r} = (\zeta^n)^q \zeta^r = \zeta^r \in U_n$$

și

$$x^{-1} = (\zeta^i)^{-1} = \zeta^{-i} = 1.\ \zeta^{-i} = \zeta^n \zeta^{-i} = \zeta^{n-i} \in U_n.$$

Deci U_n este subgrup cu n elemente al lui $(\mathbb{C}^*, \cdot)$.

2) Avem:

$$U_3 = \{1, \zeta, \zeta^2\} \qquad \text{unde } \zeta = \cos\frac{2\pi}{3} + i \sin\frac{2\pi}{3},$$

$$U_4 = \{1, \zeta, \zeta^2, \zeta^3\} \qquad \text{unde } \zeta = \cos\frac{2\pi}{4} + i \sin\frac{2\pi}{4},$$

$$U_5 = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4\} \qquad \text{unde } \zeta = \cos\frac{2\pi}{5} + i \sin\frac{2\pi}{5}.$$

Reprezentînd geometric numerele din $U_n = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$, punctele obținute sînt vîrfurile unui poligon regulat cu n laturi, cu centrul în origine și cu unul din vîrfuri pe Ox_1 (v. Fig. III.2).

§ 6. MORFISME DE GRUPURI

Numărul exemplelor de grupuri este considerabil și din acest motiv se impune o clasificare a acestora. Două grupuri G și Γ vor fi declarate ca fiind de același tip *(izotipice)* dacă sînt la fel de bogate în elemente și, mai puțin o bijecție $f : G \to \Gamma$, operațiile celor două grupuri acționează la fel asupra elementelor lui G, respectiv Γ. Mai precis:

6.1. *Definiție.* **Fie $(G, *)$ și $(\Gamma, \circ)$ două grupuri. O aplicație bijectivă $f : G \to \Gamma$ se numește *izomorfism* de grupuri dacă**

$$f(x * y) = f(x) \circ f(y), \qquad \forall x, y \in G.$$

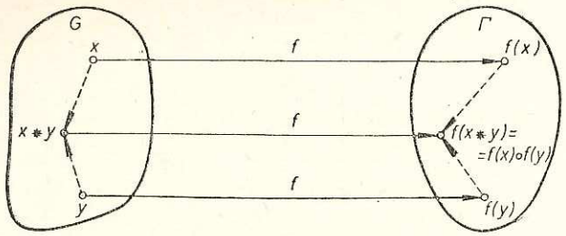


Fig. III.3

Spunem că un grup G este izomorf cu un grup Γ, și scriem $G \simeq \Gamma$, dacă există cel puțin un izomorfism $f : G \to \Gamma$. În caz contrar spunem că grupul G nu este izomorf cu grupul Γ și scriem $G \not\simeq \Gamma$.

Cu alți termeni, grupul $(G, *)$ este izomorf cu grupul $(\Gamma, \circ)$ dacă există o aplicație bijectivă $f : G \to \Gamma$ astfel încît oricare ar fi $x, y \in G$ imaginea $f(x * y)$ a compusului $x * y$ prin f este egală cu compusul $f(x) \circ f(y)$ al imaginilor prin f ale lui x și y (v. fig. III. 3); pe scurt: *imaginea compusului este egală cu compusul imaginilor.*

Dacă G și Γ sînt grupuri finite cu cîte n elemente, $G = \{a_1, a_2, \ldots, a_n\}$, $\Gamma = \{b_1, b_2, \ldots, b_n\}$ iar $f : G \to \Gamma$ este aplicația bijectivă definită prin

$$f(a_i) = b_i, \qquad 1 \leqslant i \leqslant n$$

atunci f este izomorfism dacă și numai dacă pentru orice i și j, $1 \leqslant i, j \leqslant n$, imaginea prin f a elementului $a_i * a_j$ de la intersecția liniei lui a_i cu coloana lui a_j din tabla operației lui G coincide cu elementul $b_i \circ b_j$ de la intersecția liniei lui $b_i = f(a_i)$ cu coloana lui $b_j = f(a_j)$ din tabla operației lui Γ (v. fig. III. 4).

Spunem în acest caz că tablele operațiilor celor două grupuri sînt *la fel structurate* (relativ la f).

6.2. **Teoremă. Fie $(G, *)$ și $(\Gamma, \circ)$ două grupuri. Dacă $f : G \to \Gamma$ este izomorfism, atunci și $f^{-1} : \Gamma \to G$ este izomorfism.**

Demonstrație. Fie $u, v \in \Gamma$. Cum f este aplicație bijectivă există $x, y \in G$ unic determinați astfel încît $f(x) = u$ și $f(y) = v$. Conform definiției aplicației f^{-1} avem $f^{-1}(u) = x$ și $f^{-1}(v) = y$.

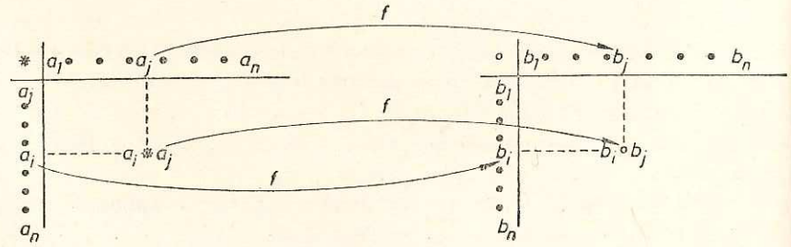


Fig. III.4

Dar

$$u \circ v = f(x) \circ f(y) = f(x * y),$$

de unde

$$f^{-1}(u \circ v) = x * y = f^{-1}(u) * f^{-1}(y)$$

și cum f^{-1} este aplicație bijectivă, rezultă că f^{-1} este izomorfism.

Exemple

1. $(\mathbf{R}, +) \simeq (\mathbf{R}_+^*, \cdot)$. *Grupul aditiv* $(\mathbf{R}, +)$ *al numerelor reale este izomorf cu grupul multiplicativ* $(\mathbf{R}_+^*, \cdot)$ *al numerelor reale strict pozitive.*

În adevăr, fie $a \in \mathbf{R}$, $a > 0$, $a \neq 1$ și $f : \mathbf{R} \to \mathbf{R}_+^*$,

$$f(x) = a^x, \qquad \forall x \in \mathbf{R}.$$

Cum f este aplicație bijectivă și

$$f(x + y) = a^{x+y} = a^x a^y = f(x)f(y), \qquad \forall x, y \in \mathbf{R},$$

rezultă că f este izomorfism.

Să observăm în acest caz că inversul izomorfismului f este aplicația $f^{-1} : \mathbf{R}_+^* \to \mathbf{R}$,

$$f^{-1}(x) = \log_a x, \qquad \forall x \in \mathbf{R}_+^*$$

și avem:

$$f^{-1}(xy) = \log_a(xy) = \log_a x + \log_a y = f^{-1}(x) + f^{-1}(y), \ \forall x, y \in \mathbf{R}_+^*.$$

Între două grupuri pot exista mai multe izomorfisme, în cazul de față chiar o infinitate (la orice $a > 0$, $a \neq 1$, corespunde un izomorfism).

2. $(\mathbf{Q}, +) \not\simeq (\mathbf{Q}_+^*, \cdot)$. *Grupul aditiv* $(\mathbf{Q}, +)$ *al numerelor raționale nu este izomorf* cu grupul multiplicativ $(\mathbf{Q}_+^*, \cdot)$ *al numerelor raționale strict pozitive.*

În adevăr, dacă $f : \mathbf{Q} \to \mathbf{Q}_+^*$ este un izomorfism între aceste două grupuri, există $r \in \mathbf{Q}$ astfel încît $f(r) = 2$. Cum $f(r/2) \in \mathbf{Q}$ și

$$2 = f(r) = f\left(\frac{r}{2} + \frac{r}{2}\right) = f\left(\frac{r}{2}\right) f\left(\frac{r}{2}\right) = \left(f\left(\frac{r}{2}\right)\right)^2$$

rezultă că $\sqrt{2} \in \mathbf{Q}$. Contradicție.

3. *Dacă* $(G, *)$ *și* $(\Gamma, \circ)$ *sînt două grupuri cu cîte trei elemente, atunci* $G \simeq \Gamma$.

Cu alte cuvinte, există un singur tip de grup cu trei elemente.

În adevăr, fie $G = \{e, a, b\}$, $\Gamma = \{\theta, u, v\}$ unde e și θ sînt elementele neutre ale lui G și Γ respectiv. Pentru că e și θ sînt elemente neutre, în tablele operațiilor celor două grupuri putem completa următoarele poziții:

$*$	e	a	b
e	e	a	b
a	a	?	?
b	b	?	?

$\circ$	θ	u	v
θ	θ	u	v
u	u	?	?
v	v	?	?

Avem $a * a = b$. În adevăr, nu putem avea $a * a = a$ căci a s-ar repeta în linia sa. De asemenea, nu putem avea $a * a = e$ căci atunci, ca să evităm repetarea lui a și e în linia lui a, am fi obligați să punem $a * b = b$, ceea ce produce o repetare a lui b în coloana acestuia.

Cum $a * a = b$, pentru a evita repetarea elementelor lui G, în liniile și coloanele tablei operației acestuia, trebuie să avem $a * b = e$, $b * a = e$, $b * b = a$. Analog, se completează tabla operației lui Γ.

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$\circ$	θ	u	v
θ	θ	u	v
u	u	v	θ
v	v	θ	u

Definind $f : G \to \Gamma$ prin $f(e) = \theta$, $f(a) = u$ și $f(b) = v$, rezultă că f este izomorfism de grupuri căci f este aplicație bijectivă și tablele operațiilor celor două grupuri sînt la fel structurate (relativ la f).

Renunțînd la condiția de bijectivitate din definiția izomorfismului se obține noțiunea mai generală de *morfism (omomorfism)* de grupuri, anume:

6.3. *Definiție.* Fie $(G, *)$ și $(\Gamma, \circ)$ **două grupuri. O aplicație** $f : G \to \Gamma$ **se numește morfism de grupuri dacă**

$$f(x * y) = f(x) \circ f(y), \qquad \forall x, y \in G.$$

Evident, orice izomorfism de grupuri este morfism de grupuri.

Aplicația $f : \mathbf{Z} \to \mathfrak{R}_4$ de la grupul $(\mathbf{Z}, +)$ la grupul $(\mathfrak{R}_4, \oplus)$,

$$f(a) = a \bmod 4, \qquad \forall a \in \mathbf{Z}$$

este un morfism de grupuri. În adevăr, dacă $a, b \in \mathbf{Z}$, fie $a_1 = a \bmod 4$, $b_1 = b \bmod 4$. Există h, $k \in \mathbf{Z}$ astfel încît:

$$a = 4h + a_1, \qquad b = 4k + b_1$$

și conform Lemei 8.1. Cap. II avem:

$$a \oplus b = a_1 \oplus b_1.$$

Rezultă că:

$$f(a + b) = (a + b) \bmod 4 = a \oplus b = a_1 \oplus b_1 = f(a) \oplus f(b), \ \forall a, b \in \mathbf{Z},$$

deci f este morfism de grupuri. Se observă că f este morfism surjectiv dar nu este injectiv.

Astfel:

$$f(7) = 7 \bmod 4 = 3 = 19 \bmod 4 = f(19).$$

6.4. **Teoremă.** **Fie** $(G, *)$ **și** $(\Gamma, \circ)$ **două grupuri,** e **și** θ **elementele neutre ale lui** G **și** Γ **respectiv. Dacă** $f : G \to \Gamma$ **este un morfism de grupuri atunci:**

1) $f(e) = \theta$;

2) $f(x') = (f(x))' \qquad \forall x \in G,$

unde x' **este simetricul lui** x **iar** $(f(x))'$ **este simetricul lui** $f(x)$.

Demonstrație. 1) Avem:

$$\theta \circ f(e) = f(e) = f(e * e) = f(e) \circ f(e)$$

și prin simplificare cu $f(e)$ se obține $\theta = f(e)$.

2) Pentru orice $x \in G$ avem:

$$\theta = f(e) = f(x * x') = f(x) \circ f(x')$$

deci $\theta = f(x) \circ f(x')$ și analog $f(x') \circ f(x) = 0$, de unde $(f(x))' = f(x')$.

Exerciții rezolvate

R—1 Fie $(G, *)$ un grup cu patru elemente astfel încît $x^2 = e$, $\forall x \in G$, unde e este elementul neutru.

1) Arătați că $G \simeq \mathfrak{K}$, unde $\mathfrak{K}$ este grupul lui Klein (v. § 3).

2) Arătați că grupul $(G, *)$ nu este izomorf cu grupul $(\mathfrak{R}_4, \oplus)$.

Soluție. 1) Fie $G = \{e, a, b, c\}$. Tablele operațiilor grupurilor G și $\mathfrak{K}$ sînt (v. § 3 și Ex. R-3, § 4):

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$\circ$	1_E	u	v	w
1_E	1_E	u	v	w
u	u	1_E	w	v
v	v	w	1_E	u
w	w	v	u	1_E

Aplicația $f : G \to \mathfrak{K}$ definită prin $f(e) = 1_E$, $f(a) = u$, $f(b) = v$ și $f(c) = w$ este izomorfism căci tablele operațiilor celor două grupuri sînt la fel structurate (relativ la f).

2) În adevăr, să presupunem că există un izomorfism $f : G \to \mathfrak{R}_4$ și fie $x \in G$ astfel f încît $(x) = 3$. Atunci:

$$0 = f(e) = f(x * x) = f(x) \oplus f(x) = 3 \oplus 3 = 2.$$

Contradicție.

R—2 Arătați că aplicația $f : \mathbf{Z} \to \mathbf{C}^*$,

$$f(h) = \cos \frac{2h\pi}{n} + i \sin \frac{2h\pi}{n}, \qquad \forall h \in \mathbf{Z}$$

este un morfism de la grupul $(\mathbf{Z}, +)$ la grupul $(\mathbf{C}^*, \cdot)$.

Determinați numerele $x \in \mathbf{Z}$ astfel încît $f(x) = 1$.

Soluție. Pentru orice h, $k \in \mathbf{Z}$ avem:

$$f(h + k) = \cos \frac{2(h + k)\pi}{n} + i \sin \frac{2(h + k)\pi}{n} = \left(\cos \frac{2h\pi}{n} + i \sin \frac{2h\pi}{n}\right) \cdot$$

$$\cdot \left(\cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}\right) = f(h) f(k)$$

și deci f este morfism de la grupul $(\mathbf{Z}, +)$ la grupul $(\mathbf{C}^*, \cdot)$.

Se observă că pentru $x \in \mathbf{Z}$ avem $f(x) = 1$ dacă și numai dacă

$$\cos \frac{2x\pi}{n} + i \sin \frac{2x\pi}{n} = 1$$

ceea ce este posibil dacă și numai dacă

$$\frac{2x\pi}{n} = 2\pi k, \qquad k \in \mathbf{Z}.$$

Rezultă că $f(x) = 1$ dacă și numai dacă $x = nk$, $k \in \mathbf{Z}$, deci $f(x) = 1$ dacă și numai dacă $n \mid x$.

R—3 Pentru orice $a \in \mathbf{R}$, definim $t_a : \mathbf{R} \to \mathbf{R}$, $t_a(x) = x + a$, $\forall x \in \mathbf{R}$.

Arătați că:

1) Mulțimea $\mathcal{T}(R) = \{t_a \mid a \in \mathbf{R}\}$ este grup în raport cu compunerea funcțiilor.

2) Grupul $(\mathbf{R}, +)$ este izomorf cu grupul $(\mathcal{T}(\mathbf{R}), \circ)$.

Soluție. 1) Pentru $a, b \in \mathbf{R}$, avem $t_a \circ t_b = t_{a+b}$. În adevăr, oricare ar fi $x \in \mathbf{R}$ avem:

$$(t_a \circ t_b)(x) = t_a(t_b(x)) = t_a(x + b) = x + b + a = t_{a+b}(x),$$

de unde $t_a \circ t_b = t_{a+b}$, deci compunerea funcțiilor induce o lege de compoziție pe $\mathcal{T}(\mathbf{R})$ evident asociativă și ca element neutru, egal cu $1_{\mathbf{R}} = t_0 \in \mathcal{T}(\mathbf{R})$.

Cum

$$t_a \circ t_{-a} = t_{a+(-a)} = t_0 = t_{(-a)+a} = t_{-a} \circ t_a, \quad \forall a \in \mathbf{R},$$

rezultă că $t_a^{-1} = t_{-a}$, $\forall a \in \mathbf{R}$, deci $(\mathcal{T}(\mathbf{R}), \circ)$ este grup.

2) Funcția $f : \mathbf{R} \to \mathcal{T}(\mathbf{R})$, $f(a) = t_a$, este bijectivă și

$$f(a + b) = t_{a+b} = t_a \circ t_b = f(a) \circ f(b), \quad \forall a, b \in \mathbf{R}.$$

Exerciții

1. Fie $M = \mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\}$.

1) Arătați că M este o parte stabilă a lui $\mathbf{C}$ în raport cu înmulțirea și că formează monoid comutativ în raport cu operația indusă.

2) Determinați elementele simetrizabile ale monoidului $(M, \cdot)$.

2. Arătați că corespondența $(x, y) \to x * y \overset{\text{def}}{=} (x + y) / (1 + xy)$ este o lege de compoziție pe intervalul $G = (-1, 1)$ și că $(G, *)$ este grup abelian.

3. Fie $\varepsilon = -1/2 + i\sqrt{3}/2$ și $G = \{1, \varepsilon, \varepsilon^2\} \subset \mathbf{C}$.

1) Arătați că G este o parte stabilă a lui $\mathbf{C}$ în raport cu înmulțirea și alcătuiți tabla operației induse.

2) Deduceți că $(G, \cdot)$ este grup abelian.

4. Fie $E = \mathbf{R} \setminus \{0\}$ și $f_i : E \to E$, $1 \leqslant i \leqslant 4$,

$$f_1(x) = x, \; f_2(x) = \frac{1}{x}, \; f_3(x) = -x, \; f_4(x) = -\frac{1}{x}, \quad \forall x \in E.$$

1) Arătați că mulțimea $G = \{f_1, f_2, f_3, f_4\}$ este stabilă în raport cu compunerea funcțiilor și alcătuiți tabla operației induse.

2) Deduceți că $(G, \circ)$ este grup abelian.

5. Fie $E = \mathbf{R} \setminus \{0, 1\}$ și $f_i : E \to E$, $1 \leqslant i \leqslant 6$,

$$f_1(x) = x, \; f_2(x) = \frac{1}{1 - x}, \; f_3(x) = \frac{x - 1}{x}, \; f_4(x) = \frac{1}{x}, \; f_5(x) = 1 - x,$$

$$f_6(x) = \frac{x}{x - 1}, \quad \forall x \in E.$$

1) Arătați că mulțimea $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ este stabilă în raport cu compunerea funcțiilor și alcătuiți tabla operației induse.

2) Deduceți că $(G, \circ)$ este grup necomutativ.

6. Fie $G = (0, \infty) \setminus \{1\}$. Arătați că corespondența

$$(x, y) \to x * y \overset{\text{def}}{=} x^{\ln y}$$

este o lege de compoziție pe G și că $(G, *)$ este grup comutativ.

7. Fie $G = [-1, \infty)$, $\Gamma = (-1, \infty)$ și următoarea lege de compoziție pe $\mathbf{R}$,

$$(x, y) \to x * y \overset{\text{def}}{=} x + y + xy.$$

1) Arătați că G și Γ sînt părți stabile ale lui $\mathbf{R}$ în raport cu legea de compoziție „$*$“.

2) Dacă „$\top$“ și „$\perp$“ sînt legile de compoziție induse pe G, respectiv Γ, de „$*$“, atunci $(G, \top)$ și $(\Gamma, \perp)$ sînt monoizi comutativi.

3) Care dintre monoizii $(G, \top)$ și $(\Gamma, \perp)$ este grup?

8. Pe $\mathbf{Z}$ se definește legea de compoziție

$$\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}, \quad (x, y) \to x \perp y \overset{\text{def}}{=} x + y - 1.$$

Arătați că $(\mathbf{Z}, \perp)$ este grup abelian.

9. Fie $(G, *)$ un grup comutativ și $a \in G$. Pe G se definește legea de compoziție

$$G \times G \to G, \quad (x, y) \to x \perp y \overset{\text{def}}{=} x * y * a.$$

Arătați că $(G, \perp)$ este grup.

10. Fie $(G, \cdot)$ un grup cu proprietatea:

$$(xy)^2 = x^2y^2, \qquad \forall x, y \in G.$$

Arătați că G este grup abelian.

11. Fie $(G, \cdot)$ un grup cu proprietatea:

$$x^2 = e, \qquad \forall x \in G$$

Arătați că G este grup abelian.

12. Fie $(G, \perp)$ și $(G, \top)$ două structuri de grup definite pe aceeași mulțime. Dacă legile de compoziție „$\perp$“ și „$\top$“ au același element neutru și

$$x \perp y = (x \top x) \top (x \top y), \quad \forall x, y \in G$$

atunci:

1) $x \perp y = x \top y$, $\forall x, y \in G$

2) $x \perp y = y \perp x$, $\forall x, y \in G$.

13. Fie $\sigma, \gamma \in \mathfrak{S}_3$, $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

Să se găsească $\xi \in \mathfrak{S}_3$ astfel încît $\sigma \circ \xi = \gamma$.

14. Fie $\sigma, \pi \in \mathfrak{S}_4$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$.

1) Arătați că $\sigma^4 = e$ și $\pi^2 = e$, unde e este permutarea identică.

2) Rezolvați în $\mathfrak{S}_4$ ecuațiile $\sigma^{129} \circ x = \pi^{101}$ și $y \circ \sigma^{207} = \pi^{53}$.

15. Fie $(G, \cdot)$ un grup și $a, b \in G$ astfel încît $ab = ba$. Să se arate că:

$$a^h b^k = b^k a^h, \qquad \forall h, k \in \mathbb{Z}.$$

16. Fie $(G, \cdot)$ un grup și e elementul său neutru. Dacă elementele $a, b \in G$ satisfac condițiile

$$b^6 = e, \qquad ab = b^4 a$$

atunci $b^3 = e$ și $ab = ba$.

17. Fie $(G, *)$ un grup și $a \in G$. Arătați că funcțiile:

$$f : G \to G, \quad f(x) = a * x, \quad \forall x \in G$$
$$g : G \to G, \quad g(x) = x * a, \quad \forall x \in G$$

sînt bijective.

18. Fie

$$H_1 = \left\{ A \in M_2(\mathbb{Z}) \;\middle|\; A = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \right\} \text{ și}$$

$$H_2 = \left\{ A \in M_2(\mathbb{Z}) \;\middle|\; A = \begin{pmatrix} 2a & 3b \\ 4c & 5d \end{pmatrix},\ a, b, c, d \in \mathbb{Z} \right\}.$$

1) Arătați că $M_2(\mathbb{Z})$ este grup în raport cu adunarea matricelor.

2) H_1 și H_2 sînt subgrupuri ale grupului $(M_2(\mathbb{Z}), +)$.

19. 1) Dacă H_1 și H_2 sînt subgrupuri ale unui grup G, atunci $H_1 \cap H_2$ este subgrup al lui G.

2) Arătați că pentru subgrupurile $3\mathbb{Z}$ și $4\mathbb{Z}$ ale grupului $(\mathbb{Z}, +)$ avem:

$$3\mathbb{Z} \cap 4\mathbb{Z} = 12\mathbb{Z}.$$

20. Fie $H = \{z \in \mathbb{C} \mid |z| = 1\}$.

1) Arătați că H este subgrup al grupului $(\mathbb{C}^*, \cdot)$;

2) Dacă U_n este grupul rădăcinilor de ordin n ale unității (v. Ex. R-2, § 5), atunci $U_n \subset H$;

3) Avem:

$$U_n \cap \mathbb{R}^* = \begin{cases} \{1\} & \text{dacă } n \text{ este impar} \\ \{1, -1\} & \text{dacă } n \text{ este par} \end{cases}$$

și

$$U_m \subset U_n \Leftrightarrow m \mid n.$$

21. Fie $f : \mathbb{R} \to \mathbb{R}$ o funcție reală cu proprietatea că există cel puțin un număr $T \in \mathbb{R}$ astfel încît

$$(*) \qquad f(x + T) = f(x), \qquad \forall x \in \mathbb{R}$$

1) Arătați că mulțimea H a numerelor reale T cu proprietatea $(*)$ este subgrup al grupului $(\mathbb{R}, +)$.

2) Determinați acest subgrup cînd

a) $f(x) = \sin 2\pi x, \qquad \forall x \in \mathbb{R}$;

b) $f(x) = \begin{cases} 1, & x \in \mathbb{Q} \\ 0, & x \in \mathbb{R} \setminus \mathbb{Q}. \end{cases}$

22. Arătați că grupul $(G, \cdot)$ de la Ex. 3 este izomorf în grupul $(\mathfrak{A}_3, \oplus)$.

23. Arătați că grupul lui Klein este izomorf cu grupul $(G, \circ)$ de la Ex. 4.

24. Arătați că grupul $(\mathfrak{S}_3, \circ)$ este izomorf cu grupul $(G, \circ)$ de la Ex. 5.

25. Arătați că funcția $f : (0, \infty) \to (-1, 1)$,

$$f(x) = \frac{x - 1}{x + 1}, \qquad \forall x \in (0, \infty)$$

este un izomorfism de la grupul $(\mathbb{R}_+^*, \cdot)$ la grupul $(G, *)$ de la Ex. 2.

26. Fie $G = \left(-\frac{\pi}{2}, \frac{\pi}{2} \right)$ și pentru orice $x, y \in G$ fie

$$x * y \overset{\text{def}}{=} \operatorname{arc\,tg}(\operatorname{tg} x + \operatorname{tg} y).$$

Arătați că $(G, *)$ este grup și că $(G, *) \simeq (\mathbb{R}, +)$.

27. Fie $\mathbf{R}_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, $\theta \in \mathbb{R}$ (v. Ex. 6, Cap. I)

și $G = \{E, A, B, C\}$, unde $E = R_0$, $A = R_{\pi/2}$, $B = R_\pi$ și $C = R_{3\pi/2}$.

1) Arătați că G este o parte stabilă a lui $M_2(\mathbb{R})$ în raport cu înmulțirea și alcătuiți tabla operației induse.

2) Deduceți că $(G, \cdot)$ este grup și arătați că $(G, \cdot) \simeq (\mathfrak{A}_4, \oplus)$.

28. Arătați că funcția $f : \mathbb{Z} \to \mathbb{Q}$, $f(k) = (-1)^k$, $\forall k \in \mathbb{Z}$, este un morfism de la grupul $(\mathbb{Z}, +)$ la grupul $(\mathbb{Q}^*, \cdot)$.

29. Fie E o mulțime cu două elemente, $E = \{a, b\}$. Pe mulțimea $\mathfrak{P}(E)$ definim legea de compoziție „Δ“,

$$X \Delta Y = (X \setminus Y) \cup (Y \setminus X), \qquad \forall X, Y \in \mathfrak{P}(E).$$

1) Alcătuiți tabla legii de compoziție „Δ“;

2) Comparați tabla operației „Δ“ cu tabla grupului $\mathfrak{K}$ al lui Klein (v. § 3) și indicați o funcție bijectivă $f : \mathfrak{K} \to \mathfrak{P}(E)$ astfel încît:

$$f(x \circ y) = f(x) \Delta f(y), \qquad \forall x, y \in \mathfrak{K};$$

3) Deduceți că $(\mathfrak{P}(E), \Delta)$ este grup.

30. Fie $E = \mathbb{R} \times \mathbb{R}$. Pentru orice $t \in \mathbb{R}$ fie funcția

$$f_t : E \to E,$$

$$f_t(x, y) = \left(x + ty + \frac{t^2}{2},\ y + t \right), \qquad \forall (x, y) \in E.$$

Arătați că:

1) $f_t \circ f_{t'} = f_{t+t'}$, $f_0 = 1_E$, $f_t^{-1} = f_{-t}$.

2) Mulțimea $G = \{f_t \mid t \in \mathbb{R}\}$ este grup în raport cu operația de compunere a funcțiilor.

3) $(G, \circ) \simeq (\mathbb{R}, +)$.

* * *

31.* Fie $R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, $S_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$,

$\theta \in \mathbb{R}$ (v. Ex. 6, Cap. I) și $G = \{E, A, B, U, V, W\}$ unde

$E = R_0$, $A = R_{2\pi/3}$, $B = R_{4\pi/3}$, $U = S_0$, $V = S_{4\pi/3}$, $W = S_{\pi/3}$

1) Arătați că G este parte stabilă a lui $M_2(\mathbf{R})$ în raport cu înmulțirea și alcătuiți tabla operației induse.

2) Deduceți că G este grup și că $(G, \cdot) \simeq (\mathfrak{S}_3, \circ)$.

32.* Fie $G = (3, \infty)$ și legea de compoziție „$*$" pe G,

$$x * y \overset{\text{def}}{=} xy - 3x - 3y + 12, \qquad \forall x, y \in G$$

1) Arătați că $(G, *)$ este grup comutativ.

2) Determinați $a, b \in \mathbf{R}$ astfel încît funcția

$$f : \mathbf{R}_+^* \to G, \qquad f(x) = ax + b, \qquad \forall x \in \mathbf{R}_+^*$$

să fie un izomorfism de la grupul $(\mathbf{R}_+^*, \cdot)$ la grupul G.

3) Arătați că

$$\underbrace{x * x * \ldots * x}_{n \text{ ori}} = (x - 3)^n + 3, \qquad \forall x \in G.$$

33.* Arătați că un grup G cu patru elemente este izomorf cu grupul lui Klein sau cu grupul $(\mathfrak{R}_1, \oplus)$.

34.* Fie $(G, \cdot)$ un grup cu un număr par de elemente. Arătați că există $a \in G$, $a \neq e$, astfel încît $a^{-1} = a$.

35.* Fie $(G, \cdot)$ un grup. Dacă pentru orice $x, y \in G$ există k astfel încît

$$(xy)^i = x^i y^i \qquad \text{pentru } i = k - 1, k, k + 1,$$

atunci G este abelian.

36.* Fie $(G, \cdot)$ un grup și H o submulțime finită a lui G. Următoarele afirmații sînt echivalente:

1) $\forall x, y \in H \Rightarrow xy \in H$;

2) H este subgrup al lui G.

37.* Fie G o mulțime și $G \times G \to G$, $(x, y) \to xy$ o lege de compoziție asociativă. Următoarele afirmații sînt echivalente:

1) $(G, \cdot)$ este grup;

2) $\forall a, b \in G$ există $x, y \in G$ astfel încît $ax = b$ și $ya = b$.

38.* Fie $(G_1, \cdot)$ și $(G_2, \cdot)$ două grupuri și $G = G_1 \times G_2$. Pe G definim legea de compoziție „$\cdot$"

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 \cdot y_1, x_2 \cdot y_2).$$

Arătați că G este grup. În ce condiții grupul G este comutativ?

39.* Fie $(G, *)$ un grup, I o mulțime și

$$G^I = \{f \mid f : I \to G\}.$$

Pe G^I definim legea de compoziție „$*$",

$$G^I \times G^I \to G^I, \qquad (f, g) \to f * g$$

unde

$$(f * g)(i) = f(i) * g(i), \qquad \forall i \in I.$$

Arătați că $(G^I, *)$ este grup. În ce condiții grupul $(G^I, *)$ este comutativ?

Cazuri particulare: a) $I = [-1, 1] \subset \mathbf{R}$, $(G, *) = (\mathbf{R}, +)$

b) $I = \mathbf{N}$, $(G, *) = (\mathbf{R}, +)$.

40.* Fie H o submulțime nevidă a lui $\mathbf{Z}$. Următoarele afirmații sînt echivalente:

1) H este subgrup al lui $\mathbf{Z}$;

2) $\exists n \geqslant 0$ astfel încît $H = n\mathbf{Z}$.

41.* Fie $(G, \cdot)$ un grup, $a \in G$ și $H_a = \{a^k \mid k \in \mathbf{Z}\}$. Arătați că:

1) H_a este subgrup al lui G.

2) H_a este finit (are doar un număr finit de elemente) dacă și numai dacă există $h, k \in \mathbf{Z}$, $h \neq k$ astfel încît $a^h = a^k$.

42.* Fie $z \in \mathbf{C}^*$ și $H_z = \{z^k \mid k \in \mathbf{Z}\}$.

Arătați că H_z este finit dacă și numai dacă există $\alpha \in \mathbf{Q}$ astfel încît $z = \cos 2\alpha\pi + i \sin 2\alpha\pi$.

43.* Pentru $a \in \mathbf{R}$, $a \neq 0$, fie $h_a : \mathbf{R} \to \mathbf{R}$, $h_a(x) = ax$, $\forall x \in \mathbf{R}$.

1) Arătați că mulțimea $\mathcal{H}(\mathbf{R}) = \{h_a \mid a \in \mathbf{R}, a \neq 0\}$ formează grup în raport cu operația de compunere a funcțiilor.

2) Arătați că $(\mathbf{R}^*, \cdot) \simeq (\mathcal{H}(\mathbf{R}), \circ)$.

44.* Fie $p > 0$ un număr prim și $H_n = U_{p^n} = \{z \in \mathbf{C} \mid z^{p^n} = 1\}$, $n = 0, 1, \ldots$

1) Arătați că $H_0 \subset H_1 \subset \ldots \subset H_n \subset \ldots \subset \mathbf{C}^*$.

2) Dacă $C_{p^\infty} = \bigcup_{n=0}^{\infty} H_n$, atunci C_{p^∞} este subgrup al lui $(\mathbf{C}^*, \cdot)$.

3) Dacă H este subgrup al lui $(C_{p^\infty}, \cdot)$, $H \neq C_{p^\infty}$, atunci există n astfel încît $H = H_n$.

§ 1. DEFINIŢIA INELULUI. EXEMPLE

Vom studia în continuare o nouă structură algebrică — structura de *inel*. Noţiunea de inel s-a degajat iniţial în cadrul teoriei numerelor, unde a apărut sub numele de *inel de numere*, prototipul fiind $\mathbf{Z}$ luat împreună cu operaţiile de adunare şi înmulţire a numerelor întregi,

$$\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z},\ (x,\ y) \to x + y,$$

respectiv

$$\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z},\ (x,\ y) \to xy.$$

Ulterior, noţiunea de inel a avut numeroase aplicaţii în diferite domenii ale Algebrei (inele de polinoame, inele de matrice), în Analiză (inele de funcţii) în Logică (inele booleene) etc.

1.1. *Definiţie.* **O mulţime nevidă A, luată împreună cu două legi de compoziţie** *(adunarea* **şi** *înmulţirea)*

$$A \times A \to A,\ (x,\ y) \to x + y$$

şi

$$A \times A \to A,\ (x,\ y) \to xy,$$

se numeşte *inel* **dacă:**

G) $(A,\ +)$ **este grup abelian.**

M) $(A,.)$ **este monoid.**

D) **înmulţirea este distributivă faţă de adunare, anume:**

$$x(y + z) = xy + xz,\ (y + z)x = yx + zx \qquad \forall\ x,\ y,\ z \in A.$$

Afirmaţia că $(A,\ +)$ este grup abelian revine la faptul că adunarea inelului satisface axiomele:

G_1) $(x + y) + z = x + (y + z) \qquad \forall\ x,\ y,\ z \in A,$

G_2) $\exists\ 0 \in A$ astfel încît $0 + x = x + 0 = x \qquad \forall\ x \in A$

G_3) $\forall\ x \in A,\ \exists\ x' \in A$ astfel încît $x' + x = x + x' = 0$

G_4) $x + y = y + x \qquad \forall\ x,\ y \in A.$

Afirmaţia că $(A,.)$ este monoid revine la faptul că înmulţirea inelului satisface axiomele:

M_1) $(xy)z = x(yz) \qquad \forall\ x,\ y,\ z \in A$

M_2) $\exists\ 1 \in A$ astfel încît $1 \cdot x = x \cdot 1 = x \qquad \forall\ x \in A$

Vom spune că $(A,\ +)$ este *grupul aditiv* al inelului A şi că $(A,\cdot)$ este *monoidul multiplicativ* al inelului A. Ansamblul de condiţii $G_1 - G_4$, M_1, M_2 şi D poartă numele de *axiomele inelului*. Elementele 0 şi 1 sînt unic determinate şi se numesc *elementul zero*, respectiv *elementul unitate* al inelului A. Inelul A se numeşte *finit* dacă A are doar un număr finit de elemente. Elementele $x \in A$ simetrizabile în raport cu înmulţirea lui A se numesc *elemente inversabile* sau *unităţi* ale inelului A.

Dacă înmulţirea inelului satisface încă axioma:

M_3) $xy = yx \qquad \forall\ x,\ y \in A$

spunem că A este *inel comutativ*.

Spunem că A este *inel fără divizori ai lui zero* dacă

$$x \neq 0 \quad \text{şi} \quad y \neq 0 \Rightarrow xy \neq 0$$

Un inel comutativ cu cel puţin două elemente şi fără divizori ai lui zero se numeşte *domeniu de integritate*.

Exemple

1. *Inelul* $\mathbf{Z}$ *al întregilor raţionali.* Din proprietăţile adunării şi înmulţirii numerelor întregi, enumerate în Cap. I, § 1, rezultă că $(\mathbf{Z},\ +,.)$ este inel comutativ, numit *inelul întregilor raţionali.*

2. *Inelul* $\mathbf{Z}[i]$ *al întregilor lui Gauss.* Fie $\mathbf{Z}[i]$ mulţimea tuturor numerelor complexe de forma $a + bi$, cu $a,\ b \in \mathbf{Z}$, numite *întregi ai lui Gauss.* Dacă $a + bi$ şi $c + di$ sînt din $\mathbf{Z}[i]$, atunci

$$(a + bi) + (c + di) = (a + c) + (b + d)\mathrm{i} \in \mathbf{Z}[\mathrm{i}]$$

şi

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)\mathrm{i} \in \mathbf{Z}[\mathrm{i}].$$

Rezultă că $\mathbf{Z}[\mathrm{i}]$ este o parte stabilă a lui $\mathbf{C}$ în raport cu adunarea şi înmulţirea numerelor complexe. Evident, operaţiile induse verifică axiomele G_1, G_4, M_1, M_3 şi D.
Cum $0 = 0 + 0 \cdot \mathrm{i}$ şi $1 = 1 + 0.\mathrm{i}$, rezultă că aceste operaţii verifică şi axiomele G_2 şi M_2. În fine, pentru orice $z \in \mathbf{Z}[\mathrm{i}]$, $z = a + \mathrm{i}b$, avem $-z = (-a) + (-b)\mathrm{i} \in \mathbf{Z}[\mathrm{i}]$, deci este verificată şi axioma G_2. Aşadar $\mathbf{Z}[\mathrm{i}]$ este inel comutativ în raport cu operaţiile induse pe $\mathbf{Z}[\mathrm{i}]$ de adunarea şi înmulţirea numerelor complexe, numit *inelul întregilor lui Gauss.*

3. *Inelul* $(\mathcal{R}_n,\ \oplus,\ *)$ *al resturilor modulo n.* Fie n un număr întreg pozitiv şi $\mathcal{R}_n = \{0,\ 1,\ 2,\ \ldots,\ n - 1\} \subset \mathbf{Z}$. Operaţiile induse pe $\mathcal{R}_n$ de adunarea şi înmulţirea modulo n satisfac axiomele inelului comutativ (v. § 8, Cap. II). Aşadar, $\mathcal{R}_n$ este inel comutativ în raport cu adunarea şi înmulţirea modulo n, numit *inelul resturilor modulo n.*

Un interes aparte, prin aplicaţiile pe care le are în diferite domenii ale tehnicii (aritmetica calculatoarelor, teoria codurilor) îl prezintă inelul $(\mathcal{R}_2,\ \oplus,\ *)$

$\oplus$	0	1
0	0	1
1	1	0

$*$	0	1
0	0	0
1	0	1

Tablele operaţiilor inelului $\mathcal{R}_2 = \{0,\ 1\}$.

În inelul $\mathcal{R}_6$ avem $2 * 3 = 0$, $4 * 3 = 0$, deci $(\mathcal{R}_6, \oplus, *)$ este inel cu divizori ai lui zero.

4. $(\mathbf{Q}, +, .)$, $(\mathbf{R}, +, .)$ și $(\mathbf{C}, +, .)$ sînt inele comutative (v. Cap. I, § 1). Să observăm că pentru orice $x \neq 0$ din $\mathbf{Q}$, $\mathbf{R}$ sau $\mathbf{C}$ există $y \neq 0$ din $\mathbf{Q}$, $\mathbf{R}$ respectiv $\mathbf{C}$, astfel încît $xy = 1$. Inelele cu această proprietate suplimentară vor fi studiate mai tîrziu.

5. *Inelul matricelor pătratice.* Fie A un inel. Inelul A poate fi oricare din inelele $\mathbf{Z}$, $\mathbf{Z}[i]$, $\mathcal{R}_n$, $\mathbf{Q}$ etc. Notăm cu $M_2(A)$ mulțimea tuturor matricelor U pătratice de ordin 2 cu coeficienți din A,

$$U = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad a_{ij} \in A.$$

Dacă $U, V \in M_2(A)$,

$$U = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad V = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

definim matricele $U + V$ și UV prin

$$U + V \stackrel{\text{def}}{=} \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix} \in M_2(A)$$

și

$$UV \stackrel{\text{def}}{=} \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix} \in M_2(A).$$

Matricele 0, E și $-U$ din $M_2(A)$,

$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad -U = \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}$$

se numesc respectiv *matricea zero*, *matricea unitate*, *opusa* matricei U.

Am amintit o serie de proprietăți ale adunării și înmulțirii matricelor din $M_2(\mathbf{R})$. Demonstrațiile multora dintre ele se fac invocînd proprietăți ale adunării și înmulțirii numerelor reale, ce sînt de asemenea adevărate pentru adunarea și înmulțirea oricărui inel A. Din acest motiv, asemenea demonstrații pot fi reproduse și pentru matricele din $M_2(A)$. Pe această cale se poate demonstra:

G_1) $(U + V) + W = U + (V + W)$,
G_2) $0 + U = U + 0 = U$,
G_3) $U + (-U) = (-U) + U = 0$,
G_4) $U + V = V + U$,
M_1) $(UV)W = U(VW)$,
M_2) $EU = UE = U$,
D) $U(V + W) = UV + UW$; $(V + W)U = VU + WU$

oricare ar fi $U, V, W \in M_2(A)$.

Rezultă că adunarea și înmulțirea matricelor conferă lui $M_2(A)$ o structură de inel.

La fel se organizează ca inel mulțimea $M_n(A)$ a matricelor pătratice de ordin n cu coeficienți din A.

Cînd $n > 1$, inelul $M_n(A)$ nu este comutativ și are divizori ai lui zero. Astfel, dacă $U, V \in M_2(\mathcal{R}_6)$,

$$U = \begin{pmatrix} 1 & 3 \\ 3 & 3 \end{pmatrix}, \quad V = \begin{pmatrix} 3 & 0 \\ 3 & 2 \end{pmatrix}$$

atunci

$$UV = \begin{pmatrix} 1 & 3 \\ 3 & 3 \end{pmatrix}\begin{pmatrix} 3 & 0 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 1*3 \oplus 3*3 & 1*0 \oplus 3*2 \\ 3*3 \oplus 3*3 & 3*0 \oplus 3*2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

deci inelul $M_2(\mathcal{R}_6)$ are divizori ai lui zero.

§ 2. REGULI DE CALCUL ÎNTR-UN INEL

Calculul algebric cu elementele unui inel beneficiază de toate regulile date pentru grupuri și monoizi, dacă sînt implicate separat adunarea, respectiv înmulțirea inelului. În afară de acestea, într-un inel avem o serie de reguli de calcul specifice, care se referă la ansamblul celor două operații ale inelului.

1. *Pentru orice* $x \in A$ *avem*: $x0 = 0x = 0$. În adevăr, fie $y = x0$. Cum $x0 = x(0 + 0) = x0 + x0$, avem $y = y + y$. Atunci:

$$0 = y + (-y) = (y + y) + (-y) = y + (y + (-y)) =$$
$$= y + 0 = y = x0$$

și analog, $0x = 0$.

2. *Într-un inel* A *cu cel puțin două elemente* avem $1 \neq 0$.

În adevăr, dacă $1 = 0$, atunci $x = 1x = 0x = 0$, de unde $A = \{0\}$. Contradicție!

3. (regula semnelor). *Oricare ar fi* $x, y \in A$ *avem*: $(-x)y = x(-y) = -xy$ și $(-x)(-y) = xy$.

În adevăr, $0 = 0y = ((-x) + x)y = (-x)y + xy = xy + (-x)y$, de unde rezultă că $(-x)y$ este opusul lui xy, deci $(-x)y = -xy$. Analog, $x(-y) = -xy$. În fine, $(-x)(-y)) = -(x(-y)) = -(-xy) = xy$.

4. (distributivitatea înmulțirii față de scădere). *Oricare ar fi* $x, y, z \in A$, *avem*: $x(y - z) = xy - xz$ *și* $(y - z)x = yx - zx$.

Reamintim că $y + (-z)$ se notează cu $y - z$. Avem:

$$x(y - z) = x(y + (-z)) = xy + x(-z) = xy - xz$$

și analog $(y - z)x = yx - zx$.

5. *Într-un inel A fără divizori ai lui zero, din $xy = xz$ sau $yx = zx$, cu $x \neq 0$, rezultă $y = z$.*

În adevăr, dacă $xy = xz$, atunci

$$x(y - z) = xy - xz = xy - xy = 0$$

și cum $x \neq 0$ rezultă că $y - z = 0$, deci $y = z$. Analog, din $yx = zx$ rezultă $y = z$.

Exerciții rezolvate

R—1 Arătați că într-un inel comutativ A avem:

1) $(a + b)(a - b) = a^2 - b^2, \qquad \forall\, a, b \in A$

2) $(a + b)^2 = a^2 + 2ab + b^2, \qquad \forall\, a, b \in A,$

unde $2ab = ab + ab$ (v. Cap. II, § 9).

Soluție. Folosim distributivitatea înmulțirii față de adunare și apoi față de scădere, avem:

$$(a + b)(a - b) = a(a - b) + b(a - b) = aa - ab + ba - bb =$$
$$= a^2 - ab + ab - b^2 = a^2 - b^2.$$

2) Conform definiției puterilor unui element și distributivității înmulțirii față de adunare, avem:

$$(a + b)^2 = (a + b)(a + b) = (a + b)a + (a + b)b =$$
$$= a^2 + ba + ab + b^2 = a^2 + ab + ab + b^2 = a^2 + 2ab + b^2.$$

R—2 Fie A un inel comutativ cu proprietatea:

(α) $\qquad a + a + a = 0, \qquad \forall\, a \in A.$

1) Arătați că $(a + b)^3 = a^3 + b^3, \qquad \forall\, a, b \in A;$

2) Arătați că inelele $\mathcal{R}_3$ și $M_2(\mathcal{R}_3)$ au proprietatea (α).

3) Fie $U, V \in M_2(\mathcal{R}_3)$,

$$U = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \quad V = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Calculați $(U + V)^3$ și $U^3 + V^3$. Explicați rezultatul.

Soluție. 1) Să arătăm la început că într-un inel comutativ este adevărată formula

$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3, \qquad \forall\, a, b \in A.$$

În adevăr, folosind rezultatul de la exercițiul precedent și Ex. R-3, Cap. II, § 9, avem:

$$(a + b)^3 = (a + b)^2(a + b) = (a^2 + 2ab + b^2)(a + b) =$$
$$= (a^2 + 2ab + b^2)a + (a^2 + 2ab + b^2)b = a^3 + 2a^2b + b^2a + a^2b + 2ab^2 + b^3 =$$
$$= a^3 + 3a^2b + 3ab^2 + b^3.$$

Dar

$$3a^2b = a^2b + a^2b + a^2b = 0$$

și analog $3ab^2 = 0$, de unde $(a + b)^3 = a^3 + b^3$.

2) În inelul $\mathcal{R}_3$ avem:

$$0 \oplus 0 \oplus 0 = (0 \oplus 0) \oplus 0 = 0 \oplus 0 = 0,$$
$$1 \oplus 1 \oplus 1 = (1 \oplus 1) \oplus 1 = 2 \oplus 1 = 0,$$
$$2 \oplus 2 \oplus 2 = (2 \oplus 2) \oplus 2 = 1 \oplus 2 = 0,$$

de unde $a \oplus a \oplus a = 0, \quad \forall\, a \in \mathcal{R}_3$.

Fie $U \in M_2(\mathcal{R}_3)$, $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ cu $a, b, c, d \in \mathcal{R}_3$.

În inelul $M_2(\mathcal{R}_3)$ avem:

$$U \oplus U \oplus U = \begin{pmatrix} a \oplus a \oplus a & b \oplus b \oplus b \\ c \oplus c \oplus c & d \oplus d \oplus d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0.$$

3) Făcînd calculele în inelul $M_2(\mathcal{R}_3)$, avem:

$$U + V = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 \oplus 1 & 0 \oplus 1 \\ 2 \oplus 0 & 1 \oplus 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}$$

$$(U + V)^2 = (U + V)(U + V) = \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 2*2 \oplus 1*2 & 2*1 \oplus 1*2 \\ 2*2 \oplus 2*2 & 2*1 \oplus 2*2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$$

$$(U + V)^3 = (U + V)^2(U + V) = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 1*2 & 1*2 \\ 2*2 & 2*1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}$$

La fel se găsește:

$$U^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad V^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Deducem că:

$$U^3 + V^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \neq \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix} = (U + V)^3,$$

rezultat datorat faptului că $M_2(\mathcal{R}_3)$ nu este inel comutativ. Mai precis, $UV \neq VU$, după cum se poate verifica:

$$UV = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1*1 \oplus 0*0 & 1*1 \oplus 0*1 \\ 2*1 \oplus 1*0 & 2*1 \oplus 1*1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}$$

$$VU = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1*1 \oplus 1*2 & 1*0 \oplus 1*1 \\ 0*1 \oplus 1*2 & 0*0 \oplus 1*1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}.$$

§ 3. INELUL CLASELOR DE RESTURI MODULO n

Fie $n > 0$ un număr întreg. Conform teoremei împărțirii cu rest, pentru orice $a \in \mathbf{Z}$ există $q, r \in \mathbf{Z}$ unic determinați astfel încît

$$a = nq + r, \qquad 0 \leqslant r < n.$$

Numărul unic determinat r din relația precedentă, numit *restul* împărțirii lui a prin n, s-a notat cu a mod n și s-a numit încă *redusul* modulo n al lui a (v. Cap. II, § 1).

Ca rezultat al împărțirii numerelor întregi prin $n > 0$ sînt posibile resturile:

$$0, 1, \ldots, r, \ldots, n-1.$$

Prin împărțirea lui a la n se obține restul r dacă și numai dacă a este de forma $nh + r$, cu $h \in \mathbf{Z}$. Mulțimile de numere

$$C_0, C_1, \ldots, C_r, \ldots, C_{n-1},$$

unde

$$\begin{aligned} C_0 &= \{a \in \mathbf{Z} \mid a \bmod n = 0\} = \{nh \mid h \in \mathbf{Z}\} = n\mathbf{Z} \\ C_1 &= \{a \in \mathbf{Z} \mid a \bmod n = 1\} = \{nh + 1 \mid h \in \mathbf{Z}\} = n\mathbf{Z} + 1 \\ &\vdots \\ C_r &= \{a \in \mathbf{Z} \mid a \bmod n = r\} = \{nh + r \mid h \in \mathbf{Z}\} = n\mathbf{Z} + r \\ &\vdots \\ C_{n-1} &= \{a \in \mathbf{Z} \mid a \bmod n = n-1\} = \{nh + n - 1 \mid h \in \mathbf{Z}\} = n\mathbf{Z} + n - 1 \end{aligned}$$

se numesc *clase de resturi* modulo n.

Așadar, un număr întreg a aparține clasei C_r dacă și numai dacă a împărțit la n dă restul r,

$$a \in C_r \Leftrightarrow a \bmod n = r.$$

În particular $r \in C_r$ pentru $r = 0, 1, \ldots, n-1$. Clasa de resturi C_r se notează de regulă cu $\hat{r}$. Așadar

$$\hat{r} = C_r = n\mathbf{Z} + r, \qquad r = 0, 1, \ldots, n-1.$$

Să notăm cu $\mathbf{Z}_n$ mulțimea claselor de resturi modulo n,

$$\mathbf{Z}_n = \{\hat{0}, \hat{1}, \hat{2}, \ldots, \widehat{n-1}\}.$$

Dacă $\hat{a}, \hat{b} \in \mathbf{Z}_n$, definim *suma* $\hat{a} + \hat{b}$ și *produsul* $\hat{a}\hat{b}$ prin:

$$\hat{a} + \hat{b} \overset{\text{def}}{=} \widehat{a \oplus b}, \qquad \hat{a}\hat{b} \overset{\text{def}}{=} \widehat{a * b}.$$

Se definesc astfel pe $\mathbf{Z}_n$, două legi de compoziție:

$$\mathbf{Z}_n \times \mathbf{Z}_n \to \mathbf{Z}_n, \ (\hat{a}, \hat{b}) \to \hat{a} + \hat{b}$$

și

$$\mathbf{Z}_n \times \mathbf{Z}_n \to \mathbf{Z}_n, \ (\hat{a}, \hat{b}) \to \hat{a}\hat{b},$$

numite *adunarea*, respectiv *înmulțirea* claselor de resturi modulo n.

Astfel, pentru $n = 6$ avem $\mathbf{Z}_6 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}\}$ și tablele adunării și înmulțirii claselor de resturi modulo 6 sînt:

$+$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{0}$
$\hat{2}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{0}$	$\hat{1}$
$\hat{3}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{4}$	$\hat{4}$	$\hat{5}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{5}$	$\hat{5}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$

$\cdot$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$
$\hat{2}$	$\hat{0}$	$\hat{2}$	$\hat{4}$	$\hat{0}$	$\hat{2}$	$\hat{4}$
$\hat{3}$	$\hat{0}$	$\hat{3}$	$\hat{0}$	$\hat{3}$	$\hat{0}$	$\hat{3}$
$\hat{4}$	$\hat{0}$	$\hat{4}$	$\hat{2}$	$\hat{0}$	$\hat{4}$	$\hat{2}$
$\hat{5}$	$\hat{0}$	$\hat{5}$	$\hat{4}$	$\hat{3}$	$\hat{2}$	$\hat{1}$

3.3. *Teoremă.* **Adunarea și înmulțirea claselor de resturi modulo n conferă mulțimii $\mathbf{Z}_n$ o structură de inel comutativ, numit** *inelul claselor de resturi modulo n.*

Demonstrație. Să verificăm axiomele inelului comutativ. În esență demonstrația se fundamentează pe faptul că $\mathfrak{R}_n = \{0, 1, 2, \ldots, n-1\}$ are o structură de inel comutativ în raport cu operațiile induse pe $\mathfrak{R}_n$ de adunarea și înmulțirea modulo n (v. Exp. 3, § 1). De exemplu, axioma D se verifică astfel:

$$\hat{a}(\hat{b} + \hat{c}) = \hat{a}\widehat{b \oplus c} = \widehat{a * (b \oplus c)} = \widehat{a * b \oplus a * c} = \widehat{a * b} + \widehat{a * c} = \hat{a}\hat{b} + \hat{a}\hat{c}$$

și la fel se arată că G_1, G_4, M_1 și M_3 sînt verificate de adunarea și înmulțirea claselor de resturi modulo n.

Cum

$$\hat{0} + \hat{a} = \widehat{0 \oplus a} = a, \quad \hat{1}\hat{a} = \widehat{1 * a} = \hat{a}, \qquad \forall\, \hat{a} \in \mathbf{Z}_n,$$

rezultă că și axiomele G_2 și M_2 sînt verificate.

În fine, avem:

$$\hat{a} + \widehat{n - a} = \widehat{a \oplus (n - a)} = \hat{0}, \qquad \forall\, \hat{a} \in \mathbf{Z}_n,$$

deci orice clasă $\hat{a} \in \mathbf{Z}_n$ este simetrizabilă în raport cu adunarea claselor de resturi modulo n

$$-\hat{a} = \widehat{n - a}, \qquad \forall\, \hat{a} \in \mathbf{Z}_n.$$

3.2. *Observație.* Clasele de resturi modulo n au fost notate cu $\hat{0}, \hat{1}, \ldots, \widehat{n-1}$. Numerele $0, 1, \ldots, n-1$ se numesc *reprezentanții canonici* ai claselor de resturi $\hat{0}, \hat{1}, \ldots, \widehat{n-1}$ respectiv.

În aplicații este adesea profitabil să descriem clasele de resturi și cu alte numere ce aparțin acestora. În acest sens, pentru orice $x \in \mathbf{Z}$ se notează cu $\hat{x}$ clasa de resturi C_r, $0 \leqslant r < n$ astfel încît $x \in C_r$; $\hat{x}$ se numește *clasa* lui x modulo n.
Așadar, prin definiție avem:

$$(\alpha) \qquad \hat{x} \overset{\text{def}}{=} \widehat{x \bmod n}, \qquad \forall\, x \in \mathbf{Z}.$$

Astfel, dacă $n = 5$, atunci

$$\widehat{32} = \widehat{32 \bmod 5} = \hat{2} \in \mathbf{Z}_5,$$

$$\widehat{-7} = \widehat{(-7) \bmod 5} = \hat{3} \in \mathbf{Z}_5,$$

$$\widehat{25} = \widehat{25 \bmod 5} = \hat{0} \in \mathbf{Z}_5.$$

Spunem că numărul întreg x este *congruent* cu y modulo n, și scriem $x \equiv y \pmod n$ dacă și numai dacă $n \mid x - y$.

Din definiția (α) rezultă că pentru orice $x, y \in \mathbf{Z}$ avem:

$$(\beta) \qquad \hat{x} = \hat{y} \Leftrightarrow x \bmod n = y \bmod n \Leftrightarrow n \mid x - y \Leftrightarrow x \equiv y \pmod n.$$

Să mai observăm că operațiile cu clase de resturi date prin reprezentanți arbitrari se pot efectua după regulile:

$$(\gamma) \qquad \hat{x} + \hat{y} = \widehat{x + y}, \qquad \hat{x}\hat{y} = \widehat{xy}, \qquad \forall\, \hat{x}, \hat{y} \in \mathbf{Z}_n.$$

În adevăr, fie $a = x \bmod n$, $b = y \bmod n$ și $h, k \in \mathbf{Z}$ astfel încît:

$$x = nh + a, \qquad y = nk + b.$$

Atunci

$$x + y = n(h + k) + (a + b), \qquad xy = n(nhk + ak + hb) + ab.$$

Cum $a \oplus b = (a + b) \bmod n$ și $a * b = (ab) \bmod n$, acum din (β) și Teorema 8.1, Cap. II rezultă:

$$\hat{x} + \hat{y} = \hat{a} + \hat{b} = \widehat{a \oplus b} = \widehat{a + b} = \widehat{x + y}$$

și

$$\hat{x}\hat{y} = \hat{a}\hat{b} = \widehat{a * b} = \widehat{ab} = \widehat{xy}.$$

Exerciții rezolvate

R—1. Fie $M_2(\mathbf{Z}_6)$ inelul matricelor pătratice de ordin 2 cu coeficienți din $\mathbf{Z}_6$ și $U, V, E, X \in M_2(\mathbf{Z}_6)$,

$$U = \begin{pmatrix} \hat{3} & \hat{5} \\ \hat{5} & \hat{4} \end{pmatrix}, \quad V = \begin{pmatrix} \hat{3} & \hat{1} \\ \hat{1} & \hat{2} \end{pmatrix}, \quad E = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix}, \quad X = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

1) Calculați $U + V$ și UV;

2) Determinați pe X astfel încît $UX = E$. Deduceți că U este element inversabil al inelului $M_2(\mathbf{Z}_6)$.

Soluție. 1) Avem:

$$U + V = \begin{pmatrix} \hat{3} & \hat{5} \\ \hat{5} & \hat{4} \end{pmatrix} + \begin{pmatrix} \hat{3} & \hat{1} \\ \hat{1} & \hat{2} \end{pmatrix} = \begin{pmatrix} \hat{3} + \hat{3} & \hat{5} + \hat{1} \\ \hat{5} + \hat{1} & \hat{4} + \hat{2} \end{pmatrix} = \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}$$

și

$$UV = \begin{pmatrix} \hat{3} & \hat{5} \\ \hat{5} & \hat{4} \end{pmatrix} \begin{pmatrix} \hat{3} & \hat{1} \\ \hat{1} & \hat{2} \end{pmatrix} = \begin{pmatrix} \hat{3}\cdot\hat{3} + \hat{5}\cdot\hat{1} & \hat{3}\cdot\hat{1} + \hat{5}\cdot\hat{2} \\ \hat{5}\cdot\hat{3} + \hat{4}\cdot\hat{1} & \hat{5}\cdot\hat{1} + \hat{4}\cdot\hat{2} \end{pmatrix} = \begin{pmatrix} \hat{2} & \hat{1} \\ \hat{1} & \hat{1} \end{pmatrix}.$$

2) Avem:

$$\begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix} = E = UX = \begin{pmatrix} \hat{3}\alpha + \hat{5}\gamma & \hat{3}\beta + \hat{5}\delta \\ \hat{5}\alpha + \hat{4}\gamma & \hat{5}\beta + \hat{4}\delta \end{pmatrix}$$

ceea ce revine la:

a) $\begin{cases} \hat{3}\alpha + \hat{5}\gamma = \hat{1} \\ \hat{5}\alpha + \hat{4}\gamma = \hat{0} \end{cases}$ și b) $\begin{cases} \hat{3}\beta + \hat{5}\delta = \hat{0} \\ \hat{5}\beta + \hat{4}\delta = \hat{1}. \end{cases}$

Să rezolvăm sistemul a). Să observăm că elementele inversabile ale inelului $\mathbf{Z}_6$ sînt $\hat{1}$ și $\hat{5}$ (v. tabla înmulțirii inelului $\mathbf{Z}_6$) și că $\hat{1}^{-1} = \hat{1}$, $\hat{5}^{-1} = \hat{5}$. Necunoscutele sistemului care au ca coeficienți elemente inversabile din $\mathbf{Z}_6$ pot fi exprimate în funcție de celelalte. Astfel, este posibil să facem aceasta cu necunoscuta α din a doua ecuație. Cum $\gamma \in \mathbf{Z}_6$, în inelul $\mathbf{Z}_6$ putem face calculul:

$$\hat{4}\gamma + \hat{2}\gamma = (\hat{4} + \hat{2})\gamma = \hat{0}\gamma = \hat{0}.$$

Așadar, adunînd pe $\hat{2}\gamma$ la fiecare termen al ecuației a doua se obține

$$\hat{5}\alpha = \hat{2}\gamma$$

de unde, prin înmulțire cu $\hat{5}^{-1} = \hat{5}$ deducem

$$\hat{5}(\hat{5}\alpha) = \hat{5}(\hat{2}\gamma)$$

deci

$$(\hat{5}\cdot\hat{5})\alpha = (\hat{5}\,\hat{2})\gamma$$

și în definitiv $\alpha = \hat{4}\gamma$. Înlocuind în prima ecuație pe α cu $\hat{4}\gamma$ aceasta devine

$$\hat{5}\gamma = \hat{1}$$

deci $\gamma = \hat{5}$ și atunci $\alpha = \hat{4}\gamma = \hat{4}\cdot\hat{5} = \hat{2}$.

Analog se rezolvă sistemul b) și se obține $\beta = \hat{5}$, $\delta = \hat{3}$, deci

$$X = \begin{pmatrix} \hat{2} & \hat{5} \\ \hat{5} & \hat{3} \end{pmatrix} \in M_2(\mathbf{Z}_6).$$

Cum

$$XU = \begin{pmatrix} \hat{2} & \hat{5} \\ \hat{5} & \hat{3} \end{pmatrix}\begin{pmatrix} \hat{3} & \hat{5} \\ \hat{5} & \hat{4} \end{pmatrix} = \begin{pmatrix} \hat{2}\cdot\hat{3}+\hat{5}\cdot\hat{5} & \hat{2}\cdot\hat{5}+\hat{5}\cdot\hat{4} \\ \hat{5}\cdot\hat{3}+\hat{3}\cdot\hat{5} & \hat{5}\cdot\hat{5}+\hat{3}\cdot\hat{4} \end{pmatrix} = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix}$$

avem $XU = E$. Analog $= UX = E$, deci U este element inversabil al inelului $M_2(\mathbf{Z}_6)$ și

$$U^{-1} = \begin{pmatrix} \hat{2} & \hat{5} \\ \hat{5} & \hat{3} \end{pmatrix}.$$

R—2 1) Fie $\hat{a} \in \mathbf{Z}_n$. Arătați că $\hat{a}$ este element inversabil al inelului $\mathbf{Z}_n$ dacă și numai dacă a este relativ prim cu n;

2) Determinați elementele inversabile ale inelului $\mathbf{Z}_9$ și rezolvați în inelul $\mathbf{Z}_9$ ecuația $\hat{7}x + \hat{3} = \hat{2}$.

Soluție. 1) Presupunem că $\hat{a}$ este inversabilă în inelul $\mathbf{Z}_n$. Atunci există $\hat{b} \in \mathbf{Z}_n$ astfel încît $\hat{a}\hat{b} = \hat{1}$. Cum

$$\widehat{ab} = \hat{a}\hat{b} = \hat{1}$$

avem $\widehat{ab} = \hat{1}$ și din proprietatea (β) rezultă că numărul $ab - 1$ se divide prin n. Există deci $k \in \mathbf{Z}$ astfel încît $ab - 1 = nk$. Așadar

$$a \cdot b + n(-k) = 1,$$

de unde $(a, n) = 1$, (v. § 4, Cap. I).

Reciproc, dacă $(a, n) = 1$, există h, $k \in \mathbf{Z}$ astfel încît $ah + nk = 1$ (v. § 4, Cap. I). Cum

$$\hat{1} = \widehat{ah + nk} = \widehat{ah} + \widehat{nk} = \widehat{ah} + \hat{0} = \hat{a}\hat{h}$$

rezultă că $\hat{a}$ este element inversabil al inelului $\mathbf{Z}_n$ și $\hat{a}^{-1} = \hat{h}$.

2) Elementele inelului $\mathbf{Z}_9$ sînt $\hat{0}, \hat{1}, \hat{2}, \ldots, \hat{8}$.
Dintre numerele 0, 1, 2, ..., 8 sînt relativ prime cu 9 numerele 1, 2, 4, 5, 7 și 8, deci elementele inversabile ale inelului $\mathbf{Z}_9$ sînt $\hat{1}, \hat{2}, \hat{4}, \hat{5}, \hat{7}$ și $\hat{8}$. Din tabla înmulțirii inelului $\mathbf{Z}_9$ se pot determina inversele acestor clase. Prezentăm o altă metodă pe cazul $a = 7$. Algoritmul lui Euclid pentru 9 și 7 este:

$$9 = 7 \cdot 1 + 2,$$

$$7 = 2 \cdot 3 + 1.$$

Ultimul rest diferit de zero este 1 și să-l reprezentăm sub forma $7h + 9k$. Din ultima egalitate avem

$$1 = 7 - 2 \cdot 3$$

și folosind și prima egalitate rezultă:

$$1 = 7 - 2 \cdot 3 = 7 - (9 - 7 \cdot 1)3 = 7 \cdot 4 + 9 \cdot (-3).$$

Avem:

$$\hat{1} = \widehat{7 \cdot 4 + 9(-3)} = \hat{7} \cdot \hat{4} + \widehat{9(-3)} = \hat{7} \cdot \hat{4} + \hat{0} \cdot \widehat{-3} = \hat{7} \cdot \hat{4},$$

deci $\hat{7}^{-1} = \hat{4}$. Ecuația dată se rezolvă astfel:

$$\hat{7}x = \hat{2} + (-\hat{3}) = \hat{2} + \hat{6} = \hat{8}$$

și atunci

$$x = \hat{7}^{-1}\hat{8} = \hat{4}\hat{8} = \widehat{4 \cdot 8} = \widehat{32} = \hat{5}.$$

§ 4. CORPURI

Un cadru ideal pentru perfectarea calculelor algebrice este dat de inelele cu proprietatea că orice element diferit de 0 este simetrizabil în raport cu înmulțirea. Asemenea inele sînt cunoscute sub numele de *corpuri*. Mai precis:

4.1. *Definiție.* **Un inel K se numește *corp* dacă $0 \neq 1$ și orice element $x \in K$, $x \neq 0$, este simetrizabil în raport cu înmulțirea:**

$$\forall\, x \in K,\ x \neq 0 \Rightarrow \exists\, x^{-1} \in K \text{ astfel încît } x^{-1}x = xx^{-1} = 1.$$

Un corp K se numește *comutativ* dacă înmulțirea sa este comutativă.

Proprietăți

1. *Corpurile nu au divizori ai lui zero.* În adevăr, dacă x, $y \in K$, $x \neq 0$ și $y \neq 0$, atunci $xy \neq 0$ căci dacă $xy = 0$ deducem

$$y = 1 \cdot y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}0 = 0,$$

deci $y = 0$. Contradicție.

2. *Elementele diferite de zero dintr-un corp formează grup față de înmulțire.* În adevăr, fie K un corp și $K^* = K \setminus 0$. Din proprietatea 1) rezultă că K^* este o parte stabilă a lui K în raport cu înmulțirea. Cum $1 \neq 0$, rezultă că $1 \in K^*$. Deducem că operația indusă pe K^* de înmulțirea lui K este asociativă și admite pe 1 ca element neutru. Fie $x \in K^*$. Atunci $x \neq 0$ și fie x^{-1} inversul său în raport cu înmulțirea lui K. Cum $x^{-1}x = 1 \neq 0$, rezultă că $x^{-1} \neq 0$, deci $x^{-1} \in K^*$. Evident, x^{-1} este inversul lui x și în raport cu operația indusă. Deci $(K^*, .)$ este grup, numit *grupul multiplicativ* al corpului K.

Exemple

1. *Corpurile* $\mathbf{Q}$, $\mathbf{R}$ *și* $\mathbf{C}$. Din proprietățile adunării și înmulțirii numerelor (v. §1, Cap. I) rezultă că $(\mathbf{Q}, +, \cdot)$, $(\mathbf{R}, +, \cdot)$ și $(\mathbf{C}, +, \cdot)$ sînt corpuri comutative, numite respectiv *corpul numerelor raționale*, *corpul numerelor reale*, *corpul numerelor complexe*.

2. *Corpurile de numere pătratice* $\mathbf{Q}(\sqrt{d})$. Fie d un întreg liber de pătrate și

$$\mathbf{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbf{Q}\}.$$

Dacă $z, w \in \mathbb{Q}(\sqrt{d})$, $z = a + b\sqrt{d}$, $w = u + v\sqrt{d}$ cu $a, b, u, v \in \mathbb{Q}$, atunci

$$z + w = (a + u) + (b + v)\sqrt{d} \in \mathbb{Q}(\sqrt{d}),$$

$$zw = (au + dbv) + (av + bu)\sqrt{d} \in \mathbb{Q}(\sqrt{d})$$

deci $\mathbb{Q}(\sqrt{d})$ este o parte stabilă a lui $\mathbb{C}$ în raport cu adunarea și înmulțirea. Observînd că $0 = 0 + 0 \cdot \sqrt{d} \in \mathbb{Q}(\sqrt{d})$, $1 = 1 + 0 \cdot \sqrt{d} \in \mathbb{Q}(\sqrt{d})$ se deduce ușor că $\mathbb{Q}(\sqrt{d})$ este inel comutativ în raport cu operațiile induse pe $\mathbb{Q}(\sqrt{d})$ de adunarea și înmulțirea lui $\mathbb{C}$. Pentru a dovedi că $\mathbb{Q}(\sqrt{d})$ este corp mai rămîne să arătăm că pentru orice $z \in \mathbb{Q}(\sqrt{d})$, $z = a + b\sqrt{d}$, $z \neq 0$, există $z' \in \mathbb{Q}(\sqrt{d})$ astfel încît $zz' = 1$.

Dacă $z \neq 0$, atunci $a \neq 0$ sau $b \neq 0$. Rezultă că $a^2 - db^2 \neq 0$ (dacă $a^2 - db^2 = 0$ și $b = 0$ deducem și $a = 0$ iar dacă $a^2 - db^2 = 0$ și $b \neq 0$ deducem $\sqrt{d} \in \mathbb{Q}$, ambele situații fiind contradictorii).

Fie

$$z' = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{d} \in \mathbb{Q}(\sqrt{d})$$

și avem:

$$zz' = 1.$$

Rezultă că $\mathbb{Q}(\sqrt{d})$ formează corp față de operațiile induse de adunarea și înmulțirea din $\mathbb{C}$, numit *corp de numere pătratice*. Astfel $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-5})$ etc. sînt corpuri de numere pătratice.

3. Inelele $(\mathbf{Z}, +, \cdot)$ și $(\mathbf{Z}_6, +, \cdot)$ nu sînt corpuri. În adevăr $2x \neq 1$ oricare ar fi $x \in \mathbf{Z}$, deci 2 nu este inversabil în raport cu înmulțirea lui $\mathbf{Z}$. În inelul $\mathbf{Z}_6$ avem $\hat{3} \cdot \hat{4} = \hat{0}$ și cum corpurile nu au divizori ai lui zero rezultă că $(\mathbf{Z}_6, +, \cdot)$ nu este corp.

4. *Corpul $\mathbf{Z}_p$ al claselor de resturi modulo p.* Fie $p > 0$ un număr prim. Atunci inelul $\mathbf{Z}_p$ este corp.

În adevăr, elementele lui $\mathbf{Z}_p$ sînt

$$\hat{0}, \hat{1}, \hat{2}, \ldots, \widehat{p-1}.$$

Pentru orice $a \in \mathbf{Z}$, $1 \leqslant a < p$ avem $(a, p) = 1$.

În adevăr, p fiind prim, singurii divizori pozitivi ai lui p sînt 1 și p. Cum $1 \leqslant a < p$, p nu divide pe a, deci a și p admit un singur divizor comun pozitiv, anume pe 1. Atunci și c.m.m.d.c. al lui a și p este egal cu 1, deci $(a, p) = 1$. Aplicînd acum rezultatul de la Ex. R—2, §3, deducem că orice clasă $\hat{a} \in \mathbf{Z}_p$, $\hat{a} \neq \hat{0}$, este inversabilă în raport cu înmulțirea, deci $\mathbf{Z}_p$ este corp. În particular $\mathbf{Z}_5$ este corp. Faptul că orice $\hat{a} \in \mathbf{Z}_5$,

$\hat{a} \neq \hat{0}$, este inversabilă în raport cu înmulțirea se observă și pe tabla înmulțirii lui $\mathbf{Z}_5$: $\hat{1}^{-1} = \hat{1}$, $\hat{2}^{-1} = \hat{3}$, $\hat{3}^{-1} = \hat{2}$, $\hat{4}^{-1} = \hat{4}$.

$+$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{0}$
$\hat{2}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{0}$	$\hat{1}$
$\hat{3}$	$\hat{3}$	$\hat{4}$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{4}$	$\hat{4}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$

Tabla adunării lui $\mathbf{Z}_5$

$\cdot$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$
$\hat{2}$	$\hat{0}$	$\hat{2}$	$\hat{4}$	$\hat{1}$	$\hat{3}$
$\hat{3}$	$\hat{0}$	$\hat{3}$	$\hat{1}$	$\hat{4}$	$\hat{2}$
$\hat{4}$	$\hat{0}$	$\hat{4}$	$\hat{3}$	$\hat{2}$	$\hat{1}$

Tabla înmulțirii lui $\mathbf{Z}_5$

Exerciții rezolvate

R—1 *Un corp cu patru elemente.* Fie $K = \mathbf{Z}_2 \times \mathbf{Z}_2$. Pe K definim legile de compoziție:

$$(\alpha, \beta) + (\gamma, \delta) \stackrel{\text{def}}{=} (\alpha + \gamma, \beta + \delta),$$

$$(\alpha, \beta)(\gamma, \delta) \stackrel{\text{def}}{=} (\alpha\gamma + \alpha\delta + \beta\delta, \alpha\gamma + \beta\delta).$$

1) Alcătuiți tablele acestor operații.

2) Arătați că aceste operații conferă lui K o structură de corp comutativ.

Soluție. 1) Să notăm elementele lui K cu 0, e, a și b, unde

$$0 = (\hat{0}, \hat{0}),\ e = (\hat{0}, \hat{1}),\ a = (\hat{1}, \hat{0}),\ b = (\hat{1}, \hat{1}).$$

Cu aceste notații pentru elementele lui K, tablele celor două operații se completează folosind definițiile date adunării și înmulțirii pe K. Astfel

$$a + b = (\hat{1}, \hat{0}) + (\hat{1}, \hat{1}) = (\hat{1} + \hat{1}, \hat{0} + \hat{1}) = (\hat{0}, \hat{1}) = e$$

$$eb = (\hat{0}, \hat{1})(\hat{1}, \hat{1}) = (\hat{0} \cdot \hat{1} + \hat{0} \cdot \hat{1} + \hat{1} \cdot \hat{1}, \hat{0} \cdot \hat{1} + \hat{1} \cdot \hat{1}) = (\hat{1}, \hat{1}) = b \quad \text{etc.}$$

$+$	0	e	a	b
0	0	e	a	b
e	e	0	b	a
a	a	b	0	e
b	b	a	e	0

$\cdot$	0	e	a	b
0	0	0	0	0
e	0	e	a	b
a	0	a	b	e
b	0	b	e	a

2) Pe tabla adunării lui K se observă că aceasta este comutativă, are ca element neutru pe 0, și orice element din K admite opus. Pe tabla înmulțirii lui K se observă că această operație este comutativă, are pe e ca element neutru și orice element din K diferit de 0 admite invers. Restul axiomelor se pot verifica pe baza definițiilor date acestor operații. O demonstrație mai elegantă se poate concepe pe ideea de la Ex. 61*, Cap. V.

R—2 1) *Teorema lui Fermat.* Fie $a, p \in \mathbf{Z}$, cu $p > 0$ număr prim care nu divide pe a. Arătați că:

$$a^{p-1} \equiv 1 \pmod{p}.$$

2) Fie $a = 149^{128}$. Calculați $a \bmod 7$.

Soluție. Fie $Z_p^* = Z_p \setminus \{\hat{0}\}$. Cum $(\mathbf{Z}_p^*, \cdot)$ este un grup comutativ, din Ex. R—2, Cap. III, rezultă:

$$(\hat{x})^{p-1} = \hat{1}, \qquad \forall \hat{x} \in \mathbf{Z}_p^*.$$

Dar cum p nu divide pe a rezultă că

$$a \bmod p \neq 0, \text{ deci}$$

$$\hat{a} = \widehat{a \bmod p} \neq \hat{0}.$$

Deducem că $\hat{a} \in \mathbf{Z}_p^*$, deci

$$\hat{1} = (\hat{a})^{p-1} = \widehat{a^{p-1}},$$

de unde $a^{p-1} \equiv 1 \pmod{p}$.

2) În corpul $\mathbf{Z}_7$ avem

$$\widehat{149} = \widehat{149 \bmod 7} = \hat{2}.$$

Cum 7 nu divide pe 2, conform teoremei lui Fermat avem

$2^6 \equiv 1 \pmod 7$. Atunci în corpul $\mathbf{Z}_7$ avem: $\hat{1} = \hat{2}^6 = (\hat{2})^6$ deci $(\hat{2})^6 = \hat{1}$.
Dar $128 = 6 \cdot 21 + 2$, deci

$$\widehat{149^{128}} = \widehat{149}^{128} = (\hat{2})^{128} = (\hat{2})^{6 \cdot 21 + 2} = ((\hat{2})^6)^{21} \cdot (\hat{2})^2 = \hat{2}^2 = \hat{4},$$

de unde $a \bmod 7 = 4$.

§ 5. MORFISME DE INELE ȘI CORPURI

Ca și în cazul grupurilor, noțiunea de izomorfism de inele (corpuri) constituie un criteriu de clasificare a inelelor (respectiv corpurilor), un criteriu de identificare a inelelor (respectiv corpurilor) cu aceleași proprietăți algebrice.

5.1. *Definiție.* **Fie A și A' două inele. O aplicație bijectivă $f : A \to A'$ se numește** *izomorfism* **de inele dacă**

$$\begin{cases} 1)\ f(x + y) = f(x) + f(y), \\ 2)\ f(xy) = f(x)f(y) \end{cases}$$

oricare ar fi $x, y \in A$.

Vom spune că inelul A este izomorf cu inelul A', și scriem $A \simeq A'$, dacă există cel puțin un izomorfism $f : A \to A'$.

Să observăm că dacă $f : A \to A'$ este un izomorfism de inele, atunci $f(1) = 1'$. În adevăr, acest lucru decurge din surjectivitatea lui f căci dacă $x' \in R'$, atunci $x' = f(x)$ cu $x \in A$, deci:

$$f(1)x' = f(1)f(x) = f(1 \cdot x) = f(x) = x' = x'f(1),$$

de unde $f(1) = 1'$.

Renunțînd la condiția de bijectivitate asupra lui f în definiția de mai sus și adăugînd cerința:

$$3)\ f(1) = 1'$$

se obține noțiunea de *morfism (omomorfism)* de inele.

Dacă $f : A \to A'$ este morfism de inele, atunci din 1) rezultă că f este morfism de la grupul $(A, +)$ la grupul $(A', +)$. Conform rezultatelor obținute pentru morfisme de grupuri, rezultă că:

$$f(0) = 0'$$

$$f(-x) = -f(x) \qquad \forall\, x \in A.$$

Cu un argument asemănător celui folosit la grupuri, se arată că dacă $x \in A$ este inversabil, atunci $f(x)$ este element inversabil al lui A' și

$$f(x^{-1}) = (f(x))^{-1}.$$

Vom spune că o aplicație $f : K \to K'$ de la un corp K la un corp K' este *izomorfism (morfism)* de corpuri dacă f este izomorfism (respectiv morfism) de inele de la K la K'.

Orice morfism de corpuri $f : K \to K'$ este injectiv. În adevăr, fie $x_1, x_2 \in K$ astfel încît $f(x_1) = f(x_2)$ și să notăm $x = x_1 - x_2$.

Avem:

$$f(x) = f(x_1 + (-x_2)) = f(x_1) + f(-x_2) = f(x_1) + (-f(x_2)) = f(x_1) + (-f(x_1)) = 0.$$

Dacă $x \neq 0$, atunci putem scrie

$$1' = f(1) = f(xx^{-1}) = f(x)f(x^{-1}) = 0'f(x^{-1}) = 0'.$$

Contradicție, căci $1' \neq 0'$. Rămîne adevărat că $x = 0$ deci $x_1 = x_2$, de unde rezultă că f este injectiv.

Dacă A este un inel, atunci ca și în cazul grupurilor, un izomorfism (morfism) $f : A \to A$ se numește *automorfism* (resp. *endomorfism*) al inelului A. Aceeași terminologie se folosește și pentru corpuri.

Exemple

1. Aplicația $f : \mathbf{Z} \to M_2(\mathbf{Z})$,

$$f(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \qquad \forall a \in \mathbf{Z}$$

este un morfism injectiv de inele. În adevăr, pentru orice $a, b \in \mathbf{Z}$ avem:

$$f(a+b) = \begin{pmatrix} a+b & 0 \\ 0 & a+b \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = f(a) + f(b)$$

$$f(ab) = \begin{pmatrix} ab & 0 \\ 0 & ab \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = f(a)\ f(b)$$

$$f(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Injectivitatea lui f este evidentă.

2. Pentru orice $z \in \mathbf{C}$, $z = a + bi$ cu $a, b \in \mathbf{R}$, notăm cu $\bar{z} = a - bi$ *conjugatul* lui z. Aplicația

$$f : \mathbf{C} \to \mathbf{C}, \qquad f(z) = \bar{z}, \qquad \forall z \in \mathbf{C}$$

este un automorfism al corpului $\mathbf{C}$. În adevăr

$$f(z+w) = \overline{z+w} = \bar{z} + \bar{w} = f(z) + f(w),$$

$$f(zw) = \overline{zw} = \bar{z}\bar{w} = f(z)\,f(w)$$

oricare ar fi $z, w \in \mathbf{C}$.

Cum $z = \bar{\bar{z}} = f(\bar{z})$, rezultă că f este surjectiv și cum orice morfism de corpuri este injectiv, deducem că f este automorfism al corpului $\mathbf{C}$.

3. Pentru orice $z \in \mathbf{Q}(\sqrt{2})$, $z = a + b\sqrt{2}$ cu $a, b \in \mathbf{Q}$, am notat cu $z^* = a - b\sqrt{2}$ conjugatul lui z. Aplicația

$$f : \mathbf{Q}(\sqrt{2}) \to \mathbf{Q}(\sqrt{2}), \qquad f(z) = z^*, \qquad \forall z \in \mathbf{Q}(\sqrt{2})$$

este automorfism al corpului $\mathbf{Q}(\sqrt{2})$. În adevăr, conform Teoremei 5.3, §5, Cap. I, avem:

$$f(z+w) = (z+w)^* = z^* + w^* = f(z) + f(w),$$

$$f(zw) = (zw)^* = z^*w^* = f(z)f(w)$$

oricare ar fi $z, w \in \mathbf{Q}(\sqrt{2})$. Cum $z = (z^*)^* = f(z^*)$, rezultă că f este surjectiv și cum orice morfism de corpuri este injectiv, deducem că f este automorfism al corpului $\mathbf{Q}(\sqrt{2})$.

Exerciții rezolvate

R—1 Fie $K = \{0, e, a, b\}$ corpul cu patru elemente de la Ex. R—1.

4. Arătați că:

1) $(x+y)^2 = x^2 + y^2$, $(xy)^2 = x^2y^2$, $\forall x, y \in K$.

2) Aplicația $f : K \to K$, $f(x) = x^2$, $\forall x \in K$ este automorfism al corpului K și $f \neq 1_K$.

3) Dacă $g \neq 1_K$ este automorfism al lui K, atunci $g = f$.

Soluție. 1) Din tabla adunării corpului K (v. § 4) rezultă că:

$$2x = x + x = 0, \qquad \forall x \in K.$$

Cum corpul K este comutativ, pentru orice $x, y \in K$ avem:

$$(x+y)^2 = (x+y)\,(x+y) = x(x+y) + y(x+y) = x^2 + xy + yx + y^2 = x^2 + xy + xy + y^2 = x^2 + (x+x)y + y^2 = x^2 + 0y + y^2 = x^2 + y^2$$

și

$$(xy)^2 = (xy)\,(xy) = x(y(xy)) = x((yx)y) = x((xy)y) = x(x(yy)) = x(xy^2) = (xx)y^2 = x^2y^2.$$

2) Folosind pct. 1, pentru orice $x, y \in K$, avem:

$$f(x+y) = (x+y)^2 = x^2 + y^2 = f(x) + f(y)$$

și

$$f(xy) = (xy)^2 = x^2y^2 = f(x)f(y).$$

Rămîne să arătăm că f este bijectiv. Folosind tabla înmulțirii corpului K (v. § 4) valorile aplicației f pot fi date prin tabelul următor:

x	0	e	a	b
$f(x) = x^2$	0	e	b	a

Se observă astfel că $f \neq 1_K$ și că f este aplicație bijectivă.

3) Cum g este morfism de corpuri avem $g(0) = 0$ și $g(e) = e$. Atunci, pentru ca $g \neq 1_K$ trebuie ca $g(a) = b$ și $g(b) = a$, de unde $g = f$.

R—2 Fie K mulțimea tuturor matricelor $U \in M_2(\mathbf{R})$ de forma

$$U = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \qquad a, b \in \mathbf{R}.$$

1) Arătați că mulțimea K este o parte stabilă a lui $M_2(\mathbf{R})$ în raport cu adunarea și înmulțirea matricelor și că operațiile induse conferă lui K o structură de corp.

2) $\mathbf{C} \simeq K$.

Soluție. 1) Fie $U, V \in K$,

$$U = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \qquad V = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}.$$

Avem:

$$U + V = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} \in K$$

și

$$UV = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix} \in K.$$

Se mai observă că

$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in K, \quad E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in K, \quad -U = \begin{pmatrix} -a & -b \\ -(-b) & -a \end{pmatrix} \in K$$

şi acum este limpede că operaţiile induse satisfac axiomele inelului.

Fie $U \in K$, $U \neq 0$, $U = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Cum $U \neq 0$, avem $a \neq 0$ sau $b \neq 0$, deci $a^2 + b^2 \neq 0$.

Fie

$$U' = \begin{pmatrix} \dfrac{a}{a^2+b^2} & \dfrac{-b}{a^2+b^2} \\ \dfrac{b}{a^2+b^2} & \dfrac{a}{a^2+b^2} \end{pmatrix} \in K.$$

O verificare imediată arată că

$$U'U = UU' = E,$$

deci U este inversabilă şi $U^{-1} = U'$. Aşadar, K este corp.

2) Fie $z \in \mathbf{C}$, $z = a + bi$ cu $a, b \in \mathbf{R}$. Definim

$$f(z) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in K.$$

Dacă $z, w \in \mathbf{C}$, $z = a + bi$, $w = c + di$, atunci

$$z + w = (a + c) + (b + d)\mathbf{i},$$
$$zw = (ac - bd) + (ad + bc)\mathbf{i}$$

deci

$$f(z + w) = \begin{pmatrix} a + c & b + d \\ -(b + d) & a + c \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = f(z) + f(w)$$

$$f(zw) = \begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = f(z)\, f(w).$$

Se mai observă că f este aplicaţie bijectivă, deci f este izomorfism, de unde $\mathbf{C} \simeq K$.

R—3 1) Dacă $f : \mathbf{Z} \to \mathbf{C}$ este un morfism de inele, atunci $f(k) = k$, $\forall k \in \mathbf{Z}$;

2) Dacă $g : \mathbf{Q} \to \mathbf{C}$ este morfism de corpuri, atunci $g(x) = x$, $\forall x \in \mathbf{Q}$;

3) Determinaţi automorfismele corpului $\mathbf{Q}(\sqrt{2})$.

Soluţie. 1) Cum f este morfism de inele, avem $f(0) = 0$ şi $f(1) = 1$. Fie $n > 1$ şi presupunem că $f(n - 1) = n - 1$. Atunci

$$f(n) = f((n - 1) + 1) = f(n - 1) + f(1) = n - 1 + 1 = n,$$

deci este demonstrat prin inducţie că

$$f(n) = n, \qquad \forall n \in \mathbf{N}.$$

Pe de altă parte

$$f(-n) = -f(n) = -n, \qquad \forall n \in \mathbf{N}$$

şi deci

$$f(k) = k, \qquad \forall k \in \mathbf{Z}.$$

2) Fie $b \in \mathbf{Z}$, $b \neq 0$. În corpul $\mathbf{Q}$ avem

$$\frac{1}{b} \cdot b = \frac{b}{b} = 1,$$

de unde $b^{-1} = 1/b$.

Dacă $x \in \mathbf{Q}$, atunci există $a, b \in \mathbf{Z}$, $b \neq 0$ astfel încît

$$x = \frac{a}{b} = a \cdot \frac{1}{b} = ab^{-1}.$$

Fie $f : \mathbf{Z} \to \mathbf{C}$, $f(k) = g(k)$, $\forall k \in \mathbf{Z}$.
Atunci, pentru orice $h, k \in \mathbf{Z}$ avem:

$$f(h + k) = g(h + k) = g(h) + g(k) = f(h) + f(k),$$
$$f(hk) = g(hk) = g(h)g(k) = f(h)g(h),$$
$$f(1) = g(1) = 1.$$

Se deduce astfel că $f : \mathbf{Z} \to \mathbf{C}$ este morfism de inele şi atunci conform pct. 1 avem

$$g(k) = f(k) = k, \qquad \forall k \in \mathbf{Z}.$$

Acum, pentru orice $x \in \mathbf{Q}$, $x = ab^{-1}$ cu $a, b \in \mathbf{Z}$, $b \neq 0$, avem:

$$g(x) = g(ab^{-1}) = g(a)g(b^{-1}) = g(a)\,(g(b))^{-1} = ab^{-1} = x.$$

3) Fie $K = \mathbf{Q}(\sqrt{2})$ şi $h : K \to K$ un morfism de corpuri. Să observăm că $h(x) = x$, $\forall x \in \mathbf{Q}$. În adevăr, definind $g : \mathbf{Q} \to \mathbf{C}$, $g(x) = h(x)$, $\forall x \in \mathbf{Q}$, atunci pentru orice $x, y \in \mathbf{Q}$ avem:

$$g(x + y) = h(x + y) = h(x) + h(y) = g(x) + g(y),$$
$$g(xy) = h(xy) = h(x)h(y) = g(x)g(y)$$
$$g(1) = h(1) = 1$$

deci g este morfism de corpuri. Aplicînd pct. 2 rezultă

$$h(x) = g(x) = x, \qquad \forall x \in \mathbf{Q}.$$

Caz. I: $h(\sqrt{2}) = \sqrt{2}$. Dacă $z \in \mathbf{Q}(\sqrt{2})$, $z = a + b\sqrt{2}$ cu $a, b \in \mathbf{Q}$, atunci

$$h(z) = h(a + b\sqrt{2}) = h(a) + h(b\sqrt{2}) = h(a) + h(b)\,h(\sqrt{2}) = a + b\sqrt{2} = z,$$

de unde $h = 1_K$.

Caz. II: $h(\sqrt{2}) \neq \sqrt{2}$. Să arătăm că $h(\sqrt{2}) = -\sqrt{2}$.

În adevăr,

$$2 = h(2) = h((\sqrt{2})^2) = (h(\sqrt{2}))^2$$

şi cum $h(\sqrt{2}) \in \mathbf{Q}(\sqrt{2}) \subset \mathbf{R}$, $h(\sqrt{2}) \neq \sqrt{2}$, deducem că $h(\sqrt{2}) = -\sqrt{2}$.

Fie acum $z \in \mathbf{Q}(\sqrt{2})$, $z = a + b\sqrt{2}$ cu $a, b \in \mathbf{Q}$.

Avem:

$$h(z) = h(a + b\sqrt{2}) = h(a) + h(b\sqrt{2}) = h(a) + h(b)\,h(\sqrt{2}) = a - b\sqrt{2}.$$

Aşadar corpul $K = \mathbf{Q}(\sqrt{2})$ are două automorfisme (v. Exp. 3).

Notă istorică. Nu am dat pînă acum un exemplu de corp necomutativ. În realitate acest lucru este dificil. Primul exemplu de corp necomutativ a fost dat de către W.R. Hamilton în 1843, după circa zece ani de căutări. Vom da o „copie matriceală" (via un izomorfism de corpuri) a exemplului lui Hamilton.

Fie H mulțimea matricelor din $M_2(\mathbf{C})$ de forma

$$\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \quad z, w \in \mathbf{C}.$$

Un calcul asemănător cu cel de la Ex. R-2) arată că H este o parte stabilă a lui $M_2(\mathbf{C})$ în raport cu adunarea și înmulțirea matricelor. Se verifică că H este inel în raport cu operațiile induse. Fie $U \in H$,

$$U = \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \neq 0, \quad z = a + ib, \quad w = c + id.$$

Atunci $\Delta \overset{\text{def}}{=} \det(U) = z\bar{z} + w\bar{w} = a^2 + b^2 + c^2 + d^2 \neq 0$. Cum

$$U' \overset{\text{def}}{=} \begin{pmatrix} \frac{\bar{z}}{\Delta} & -\frac{w}{\Delta} \\ \frac{\bar{w}}{\Delta} & \frac{z}{\Delta} \end{pmatrix} \in H$$

și $U'U = UU' = E$, rezultă că orice matrice $U \in H$, $U \neq 0$ este inversabilă în raport cu înmulțirea lui H, deci H este corp.

Matricele

$$\alpha = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad \beta = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \gamma = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

sînt din H și se verifică ușor că

$$\alpha^2 = \beta^2 = \gamma^2 = -E$$

$$\beta\alpha = -\beta\alpha = \gamma, \ \beta\gamma = -\gamma\beta = \alpha, \ \gamma\alpha = -\alpha\gamma = \beta.$$

În particular rezultă că H este corp necomutativ, numit *corpul cuaternionilor reali.*

Un alt rezultat important în legătură cu problema discutată a fost dat în 1905 de către J.H.M. Wedderburn, care a demonstrat că orice corp finit este comutativ. Se poate arăta că numărul elementelor unui corp finit este de forma p^n, cu p prim și $n \geqslant 1$. Reciproc, pentru orice număr de forma p^n, p prim și $n \geqslant 1$, există, mai puțin un izomorfism de corpuri, un singur corp F_{p^n} cu p^n elemente. Corpurile finite au aplicații spectaculoase în diferite domenii ale matematicii și tehnicii.

Exerciții

1. Pe mulțimea $A = \mathbf{Z} \times \mathbf{Z}$ definim legile de compoziție:

$$(a, b) + (c, d) \overset{\text{def}}{=} (a + b, c + d)$$

$$(a, b)\ (c, d) \overset{\text{def}}{=} (ac + 3bd, ad + bc).$$

Arătați că aceste legi de compoziție conferă mulțimii A o structură de inel comutativ și fără divizori ai lui zero.

2. Pe mulțimea $\mathbf{Z}$ a numerelor întregi definim legile de compoziție:

$$x \perp y \overset{\text{def}}{=} x + y + 3, \qquad \forall x, y \in \mathbf{Z}$$

$$x \top y \overset{\text{def}}{=} xy + 3x + 3y + 6, \quad \forall x, y \in \mathbf{Z}.$$

Arătați că:

1) $(\mathbf{Z}, \perp)$ este grup abelian.
2) $(\mathbf{Z}, \top)$ este monoid comutativ.
3) $x \top (y \perp z) = (x \top y) \perp (x \top z), \qquad \forall x, y, z \in \mathbf{Z}.$

Deduceți că $(\mathbf{Z}, \perp, \top)$ este inel comutativ fără divizori ai lui zero. Determinați elementele inversabile ale acestui inel.

3. Fie $a \in \mathbf{Z}$ și $f : \mathbf{Z} \to \mathbf{Z}$, $f(x) = x - a, \qquad \forall x \in \mathbf{Z}.$

1) Arătați că se pot defini în mod unic două legi de compoziție „$\perp$" și „$\top$" pe $\mathbf{Z}$ astfel încît:

$$f(x + y) = f(x) \perp f(y), \qquad \forall x, y \in \mathbf{Z},$$

$$f(xy) = f(x) \top f(y), \qquad \forall x, y \in \mathbf{Z}.$$

2) Arătați că $(\mathbf{Z}, \perp, \top)$ este inel comutativ și fără divizori ai lui zero, elementele sale inversabile fiind $1 - a$, $-1 - a$.

3) Cînd $a = 3$, comparați rezultatul cu cel de la Ex. 2.

4. Fie

$$A = \left\{ \begin{pmatrix} a & b \\ 5b & a \end{pmatrix} \;\middle|\; a, b \in \mathbf{Z} \right\}.$$

Arătați că A este o parte stabilă a lui $M_2(\mathbf{Z})$ în raport cu adunarea și înmulțirea matricelor și că formează inel comutativ și fără divizori ai lui zero în raport cu operațiile induse.

5. Pe mulțimea $A = \mathbf{Z} \times \mathbf{Z}$ definim legile de compoziție:

$$(a, b) + (c, d) \overset{\text{def}}{=} (a + c, b + d),$$

$$(a, b)\ (c, d) \overset{\text{def}}{=} (ac, bd).$$

Arătați că aceste legi de compoziție conferă mulțimii A o structură de inel comutativ cu divizori ai lui zero. Care sînt elementele inversabile ale acestui inel?

6. Fie A_1 și A_2 două inele. Pe mulțimea $A = A_1 \times A_2$ definim legile de compoziție:

$$(a_1, a_2) + (b_1, b_2) \overset{\text{def}}{=} (a_1 + b_1, a_2 + b_2),$$

$$(a_1, a_2)\ (b_1, b_2) \overset{\text{def}}{=} (a_1 b_1, a_2 b_2).$$

1) Arătați că A are o structură de inel în raport cu aceste legi de compoziție (A este numit *produsul direct* al lui A_1 cu A_2).

2) Arătați că A este comutativ dacă și numai dacă A_1 și A_2 sînt inele comutative.

7. Fie $(\mathcal{R}_9, \oplus, *)$ inelul resturilor modulo 9 și $A = \mathcal{R}_9 \times \mathbf{Z}$ produsul direct al inelului $\mathcal{R}_9$ cu inelul $\mathbf{Z}$ (v. Ex. 6).

1) Enumerați elementele inversabile ale inelului A.

2) Cum pot fi caracterizate elementele inversabile ale produsului direct al două inele?

8. Fie $(\mathcal{R}_2, \oplus, *)$ inelul resturilor modulo 2 și $B = \mathcal{R}_2 \times \mathcal{R}_2$ produsul direct al inelului $\mathcal{R}_2$ cu $\mathcal{R}_2$.

1) Alcătuiți tabla adunării și tabla înmulțirii inelului B.

2) Deduceți că $x + x = 0$ și $x^2 = x, \quad \forall x = (x_1, x_2) \in B$.

9. Fie B un inel astfel încît $x^2 = x, \quad \forall x \in B$. Arătați că:

1) $x + x = 0, \quad \forall x \in B.$

2) $xy = yx, \qquad \forall x, y \in B.$

10. Fie $(\mathcal{R}_2, \oplus, *)$ inelul resturilor modulo 2.

1) Cîte elemente are inelul $M_2(\mathcal{R}_2)$?

2) Arătați că $U + U = 0$, $\forall U \in M_2(\mathcal{R}_2)$.

3) Indicați matricele inversabile ale acestui inel și determinați inversele lor.

11. Fie A mulțimea tuturor șirurilor de numere reale. Pe mulțimea A definim legile de compoziție:

$$(a_0, a_1, ..., a_n, ...) + (b_0, b_1, ..., b_n, ...) = (a_0 + b_0, a_1 + b_1, ..., a_n + b_n, ...)$$
$$(a_0, a_2, ..., a_n, ...)\ (b_0, b_1, ..., b_n, ...) = (a_0b_0, a_1b_1, ..., a_nb_n, ...).$$

1) Arătați că aceste legi de compoziție conferă mulțimii A o structură de inel comutativ cu divizori ai lui zero. Care sînt elementele inversabile ale acestui inel?

2) Arătați că mulțimea B a șirurilor mărginite (resp. convergente) este o parte stabilă a lui A în raport cu adunarea și înmulțirea și că formează inel în raport cu operațiile induse.

12. Arătați că într-un inel comutativ A avem:

$$a^n - b^n = (a - b)\ (a^{n-1} + a^{n-2}b + ... + b^{n-1}), \qquad \forall a, b \in A.$$

13. Arătați că într-un inel comutativ A este valabilă formula binomului lui Newton:

$$(a + b)^n = \sum_{k=0}^{n} C_n^k\ a^{n-k}b^k, \qquad \forall a, b \in A.$$

14. Fie $(\mathcal{R}_5, \oplus, *)$ inelul resturilor modulo 5.

1) Verificați că $a \oplus a \oplus a \oplus a \oplus a = 0$, $\qquad \forall a \in \mathcal{R}_5$.

2) Deduceți, folosind formula binomului lui Newton, că:

$$(a \oplus b)^5 = a^5 \oplus b^5 \qquad \forall a, b \in \mathcal{R}_5.$$

15. Fie $U \in M_3(\mathbf{R})$,

$$U = \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix}, \quad a, b, c \in \mathbf{R}.$$

1) Pentru ce numere $a, b, c \in \mathbf{R}$ avem $U^2 = 0$?

2) Dacă $U^2 = 0$, atunci $E - U$ este inversabilă și $(E - U)^{-1} = E + U$.

16. Fie $\mathbf{Z}_{12}$ inelul claselor de resturi modulo 12 și G mulțimea elementelor inversabile ale acestui inel.

1) Determinați elementele lui G și arătați că G este o parte stabilă în raport cu înmulțirea lui $\mathbf{Z}_{12}$.

2) Alcătuiți tabla operației induse și deduceți că $(G, \cdot)$ este grup izomorf cu grupul lui Klein.

17. Rezolvați următorul sistem de ecuații liniare cu coeficienți în inelul $\mathbf{Z}_{12}$:

$$\begin{cases} \hat{3}x + \hat{2}y = \hat{4}, \\ \hat{2}x + \hat{3}y = \hat{1}. \end{cases}$$

18. Fie $U \in M_2(\mathbf{Z}_{12})$, $\qquad U = \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{c} & \hat{d} \end{pmatrix}$ și $\hat{e} = \hat{a}\hat{d} - \hat{c}\hat{b} = \det(U)$.

1) Arătați că matricea U este element inversabil al inelului $M_2(\mathbf{Z}_{12})$ dacă și numai dacă $\det(U)$ este egal cu $\hat{1}$, $\hat{5}$, $\hat{7}$, sau $\hat{11}$ și,

$$U^{-1} = \hat{e}^{-1}\begin{pmatrix} \hat{d} & -\hat{b} \\ -\hat{c} & \hat{a} \end{pmatrix}.$$

2) Următoarele matrice din $M_2(\mathbf{Z}_{12})$ sînt inversabile și găsiți inversele lor:

$$U = \begin{pmatrix} \hat{2} & \hat{1} \\ \hat{1} & \hat{3} \end{pmatrix}, \quad V = \begin{pmatrix} \hat{5} & \hat{4} \\ \hat{1} & \hat{3} \end{pmatrix}, \quad W = \begin{pmatrix} \hat{2} & \hat{1} \\ \hat{1} & \hat{1} \end{pmatrix}.$$

19. Pe mulțimea $K = \mathbf{Q} \times \mathbf{Q}$ definim legile de compoziție:

$$(a, b) + (c, d) = (a + c, b + d),$$
$$(a, b)\ (c, d) = (ac - bd, ad + bc + bd).$$

Arătați că aceste operații conferă lui K o structură de corp comutativ.

20. Pe mulțimea $K = \mathbf{R} \times \mathbf{R}$ definim legile de compoziție:

$$(a, b) + (c, d) = (a + c, b + d),$$
$$(a, b)\ (c, d) = (ac - bd, ad + bc).$$

Arătați că aceste operații conferă mulțimii K o structură de corp comutativ.

21. Pe intervalul $K = (0, \infty)$ definim legile de compoziție:

$$x \perp y = xy, \qquad \forall x, y \in K,$$
$$x \top y = x^{\ln y}, \qquad \forall x, y \in K.$$

Arătați că tripletul $(K, \perp, \top)$ este un corp comutativ.

22. Fie $L = \{0, E, U, V\}$, unde $0, E, U, V \in M_2(\mathbf{Z}_2)$,

$$0 = \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}, \quad E = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix}, \quad U = \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{1} & \hat{1} \end{pmatrix}, \quad V = \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{1} & \hat{0} \end{pmatrix}.$$

1) Arătați că L este o parte stabilă a lui $M_2(\mathbf{Z}_2)$ în raport cu operațiile de adunare și înmulțire și alcătuiți tablele operațiilor induse.

2) Deduceți că $(L, +, \cdot)$ este un corp comutativ.

23. Fie $L = \left\{ \begin{pmatrix} \hat{a} & \hat{b} \\ -\hat{b} & \hat{a} \end{pmatrix} \;\middle|\; \hat{a}, \hat{b} \in \mathbf{Z}_3 \right\}$.

1) Arătați că $\hat{x}^2 + \hat{y}^2 \neq \hat{0}$, $\qquad \forall \hat{x}, \hat{y} \in \mathbf{Z}_3$, $\hat{x} \neq \hat{0}$ sau $\hat{y} \neq \hat{0}$.

2) Arătați că L este o parte stabilă a lui $M_2(\mathbf{Z}_3)$ în raport cu adunarea și înmulțirea și că formează corp comutativ cu 9 elemente față de operațiile induse.

24. Pe mulțimea $A = \mathbf{Z} \times \mathbf{Z}$ definim legile de compoziție:

$$(a, b) + (c, d) = (a + c, b + d),$$
$$(a, b)\ (c, d) = (ac - bd, ad + bc).$$

1) Arătați că A are o structură de inel comutativ în raport cu aceste legi de compoziție.

2) Determinați elementele inversabile ale inelului A.

3) Arătați că $A \simeq Z[i]$.

25. Arătați că funcția $f : \mathbf{Q}(\sqrt{-3}) \to K$,

$f(z) = (a - b, 2b)$, $\forall z \in \mathbf{Q}(\sqrt{-3})$, $z = a + b\sqrt{-3}$ cu $a, b \in \mathbf{Q}$ este un izomorfism de la corpul $\mathbf{Q}(\sqrt{-3})$ la corpul K de la Ex. 19.

26. Arătați că corpul $\mathbb{C}$ este izomorf cu corpul K de la Ex. 20.

27. Arătați că corpul $\mathbf{R}$ este izomorf cu corpul K de la Ex.21.

28. Arătați că corpul L de la Ex. 22 este izomorf cu corpul K de la Ex. R-1, 4.

29. Fie $K = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \;\middle|\; a,\ b \in \mathbf{Q} \right\}$.

1) Arătați că mulțimea K este o parte stabilă a lui $M_2(\mathbf{Q})$ în raport cu adunarea și înmulțirea și că formează corp în raport cu operațiile induse.

2) Arătați că $\mathbf{Q}(\sqrt{2}) \simeq K$.

30. Fie $a, b, c \in \mathbf{R}$. Pe $\mathbf{R}$ definim legile de compoziție:

$$x \perp y = ax + by - 2, \qquad \forall x, y \in \mathbf{R}$$

$$x \top y = xy - 2x - 2y + c, \qquad \forall x, y \in \mathbf{R}.$$

1) Determinați a, b, c astfel încît $(\mathbf{R}, \perp, \top)$ să fie corp.

2) Determinați apoi $\alpha, \beta \in \mathbf{R}$ astfel încît funcția:

$$f : \mathbf{R} \to \mathbf{R}, f(x) = \alpha x + \beta, \qquad \forall x \in \mathbf{R}$$

să stabilească un izomorfism de la corpul $(\mathbf{R}, +, \cdot)$ al numerelor reale la corpul $(\mathbf{R}, \perp, \top)$.

* * *

31.* Fie A un inel și $Z(A) = \{a \in A \mid ax = xa, \quad \forall x \in A\}$.

1) Arătați că $Z(A)$ este o parte stabilă a lui A în raport cu adunarea și înmulțirea și că formează inel în raport cu operațiile induse.

2) Dacă $x^2 - x \in Z(A), \quad \forall x \in A$, atunci A este inel comutativ.

3) Determinați $Z(A)$ cînd $A = M_2(\mathbf{R})$.

32.* Fie A un inel și $U(A)$ mulțimea elementelor sale inversabile.

1) Arătați că $U(A)$ este o parte stabilă a lui A în raport cu înmulțirea și că formează grup în raport cu operația indusă.

2) Dacă A este produsul direct al inelului A_1 cu A_2 (v. Ex. 6) arătați că $U(A) = U(A_1) \times U(A_2)$.

3) Dacă A este produs al inelului $\mathbf{Z}_4$ cu inelul $\mathbf{Z}_9$, determinați elementele grupului $U(A)$.

33.* Pentru $n > 1$ notăm cu $\varphi(n)$ numărul acelor $r \in \mathbf{Z}$ astfel încît $1 \leqslant r < n$ și $(r, n) = 1$ (*indicatorul lui Euler* al lui n).

1) *(teorema lui Euler)* Pentru orice $a \in Z$, $(a, n) = 1$,

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

2) Pentru orice $a \in Z_n$, $(a, n) = 1$, avem:

$$(\hat{a})^{-1} = (\hat{a})^{\varphi(n)-1}.$$

3) Determinați elementele grupului $U(\mathbf{Z}_9)$.

34. Fie $m_1 > 1$, $m_2 > 1$ și $m = m_1 m_2$, unde $(m_1, m_2) = 1$.

1) Pentru $a \in \mathbf{Z}$ avem $(a, m) = 1 \Leftrightarrow (a, m_1) = 1$ și $(a, m_2) = 1$.

2) Deduceți că $\varphi(m) = \varphi(m_1)\varphi(m_2)$.

3) Calculați $\varphi(15)$, $\varphi(pq)$, $\varphi(p^2 \cdot q^3)$, unde p și q sînt numere prime, $p > 0$, $q > 0$, $p \neq q$.

35.* Găsiți soluțiile întregi ale ecuației $3x + 5y = 2$.

36.* Fie $n > 1$ și $\varphi_n : \mathbf{Z} \to \mathcal{R}_n$, $\varphi_n(x) = x \bmod n, \quad \forall x \in \mathbf{Z}$.

1) Arătați că φ_n este morfism surjectiv de la inelul $(Z, +, \cdot)$ la inelul $(\mathcal{R}_n, \oplus, *)$

2) Dacă $f : \mathbf{Z} \to \mathcal{R}_n$ este un morfism de inele, atunci $f = \varphi_n$.

37.* Fie $n > 1$ și $\psi_n : \mathbf{Z} \to \mathbf{Z}_n$, $\psi_n(x) = \hat{x}, \quad \forall x \in \mathbf{Z}$.

1) Arătați că ψ_n este morfism surjectiv de inele.

2) Dacă $f : \mathbf{Z} \to \mathbf{Z}_n$ este un morfism de inele, atunci $f = \psi_n$.

38.* Arătați că $(\mathcal{R}_n, \oplus, *) \simeq (\mathbf{Z}_n, +, \cdot)$.

39.* Fie $m > 1$ și $n > 1$ două numere întregi. Arătați că aplicația

$$f : \mathcal{R}_m \to \mathcal{R}_n, \quad f(a) = a \bmod n, \quad \forall a \in \mathcal{R}_m$$

este morfism de inele dacă și numai dacă $m \geqslant n$, și $n \mid m$.

40.* Fie $\mathbf{R}$ corpul numerelor reale și $f : \mathbf{R} \to \mathbf{R}$ un morfism de corpuri. Arătați că $f = 1_{\mathbf{R}}$.

§ 1. INELE DE POLINOAME

1. Construcția unui inel de polinoame. Fie A un inel comutativ. Inelul A poate fi: inelul $\mathbf{Z}$ al întregilor raționali, inelul $\mathbf{Z}_n$ al claselor de resturi modulo n etc. Inelul A poate fi în particular un corp comutativ, cum este cazul lui $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ și $\mathbf{Z}_p$, p număr prim.

Să notăm cu B mulțimea tuturor șirurilor

$$f = (a_0, a_1, a_2, \ldots), \ a_i \in A$$

care au numai un număr finit de termeni diferiți de 0. Aceasta revine la faptul că există un rang m (care depinde în genere de șirul f) astfel încît $a_i = 0$, $\forall i > m$.

Dacă $f, g \in B$, $f = (a_0, a_1, a_2, \ldots)$, $g = (b_0, b_1, b_2, \ldots)$, atunci:

$$f = g \overset{\text{def}}{\Leftrightarrow} a_i = b_i, \quad i = 0, 1, 2, \ldots,$$

$$f + g \overset{\text{def}}{\Leftrightarrow} (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots)$$

și

$$fg \overset{\text{def}}{=} (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \ldots).$$

Așadar, dacă $f + g = (s_0, s_1, s_2, \ldots)$ și $fg = (p_0, p_1, p_2, \ldots)$ atunci:

$$s_i = a_i + b_i \qquad i = 0, 1, 2, \ldots$$

și

$$p_k = a_0b_k + a_1b_{k-1} + \ldots + a_kb_0 = \sum_{i+j=k} a_ib_j, \qquad k = 0, 1, 2, \ldots .$$

Să observăm că dacă $f, g \in B$, atunci $f + g \in B$ și $fg \in B$. În adevăr, există $m, n \in \mathbf{N}$ astfel încît $a_i = 0$ pentru $i > m$ și $b_j = 0$ pentru $j > n$, de unde

$$s_i = a_i + b_i = 0, \qquad \text{pentru } i > \max\{m, n\}$$

și

$$c_k = \sum_{i+j=k} a_ib_j = 0, \qquad \text{pentru } k > m + n$$

după cum ușor se poate constata.

Am definit astfel pe mulțimea B două legi de compoziție:

$$B \times B \to B, \ (f, g) \to f + g$$

și

$$B \times B \to B, \ (f, g) \to fg.$$

Astfel, dacă $A = \mathbf{Z}$, $f = (-2, 3, 0, 0, \ldots)$, $g = (3, 0, 5, 0, \ldots)$, atunci

$$f + g = (-2 + 3, 3 + 0, 0 + 5, 0 + 0, \ldots) = (1, 3, 5, 0, \ldots)$$

și

$$fg = (p_0, p_1, p_2, \ldots) = (-6, 9, -10, 15, 0, \ldots)$$

căci

$$p_0 = a_0b_0 = (-2) \times 3 = -6,$$
$$p_1 = a_0b_1 + a_1b_0 = (-2) \times 0 + 3 \times 3 = 9,$$
$$p_2 = a_0b_2 + a_1b_1 + a_2b_0 = (-2) \times 5 + 3 \times 0 + 0 \times 3 = -10,$$
$$p_3 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 = (-2) \times 0 + 3 \times 5 + 0 \times 3 + 0 \times 1 = 15,$$
$$p_4 = 0$$
$$\ldots\ldots$$

Mulțimea B formează inel comutativ în raport cu legile de compoziție definite mai sus. În adevăr, dacă $f, g, h \in B$,

$$f = (a_0, a_1, \ldots), \ g = (b, b_1, \ldots), \ h = (c_0, c_1, \ldots)$$

atunci

$$(f + g) + h = (a_0 + b_0, a_1 + b_1, \ldots) + (c_0, c_1, \ldots) = ((a_0 + b_0) + c_0, (a_1 + b_1) + c_1, \ldots)$$

și

$$f + (g + h) = (a_0, a_1, \ldots) + (b_0 + c_0, b_1 + c_1, \ldots) = (a_0 + (b_0 + c_0), a_1 + (b_1 + c_1), \ldots).$$

Cum adunarea inelului A este asociativă, avem:

$$(a_i + b_i) + c_i = a_i + (b_i + c_i), \qquad i = 0, 1, \ldots$$

de unde

$$(f + g) + h = f + (g + h), \qquad \forall f, g, h \in B.$$

Analog se arată că

$$f + g = g + f, \qquad \forall f, g \in B.$$

Dacă $0 = (0, 0, \ldots)$, atunci

$$0 + f = (0 + a_0, 0 + a_1, \ldots) = (a_0, a_1, \ldots) = f = f + 0, \quad \forall f \in B,$$

deci 0 este element neutru pentru adunarea definită pe B.

În fine, dacă $f \in B$, $f = (a_0, a_1, \ldots)$, fie

$$-f \overset{\text{def}}{=} (-a_0, -a_1, \ldots)$$

și avem:

$$f + (-f) = (a_0 + (-a_0), a_1 + (-a_1), \ldots) = (0, 0, \ldots) = 0 = (-f) + f,$$

deci $(B, +)$ este grup abelian.

Se verifică imediat că operația multiplicativă $B \times B \to B$, $(f, g) \to fg$ este comutativă și admite ca element de efect nul șirul $(1, 0, 0, \ldots)$. Să verificăm că operația multiplicativă este asociativă și că este distributivă față de cea aditivă. În adevăr, dacă $f, g, h \in B$, $f = (a_0, a_1, a_2, \ldots)$

$$g = (b_0, b_1, b_2, \ldots), \quad h = (c_0, c_1, c_2, \ldots)$$

și dacă

$$(fg)h = (d_0, d_1, d_2, \ldots), \quad f(gh) = (d'_0, d'_1, d'_2, \ldots)$$

atunci:

$$d_l = \sum_{s+k=l} (\sum_{i+j=s} a_i b_i) c_k = \sum_{(i+j)+k=l} (a_i b_j) c_k$$

și

$$d'_l = \sum_{i+t=l} a_i (\sum_{j+k=t} (b_j c_k) = \sum_{i+(j+k)=l} (a_i (b_j c_k).$$

Rezultă că $d_l = d'_l$, $l = 0, 1, 2, \ldots$, de unde

$$(fg)h = f(gh), \qquad \forall f, g, h \in B.$$

De asemenea,

$$\sum_{i+j=k} a_i(b_j + c_j) = \sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_j, \qquad k = 0, 1, 2, \ldots$$

de unde

$$f(g + h) = fg + fh, \qquad \forall f, g, h \in B.$$

Elementele inelului B se numesc *polinoame* cu coeficienți în A. Dacă $f \in B$, $f = (a_0, a_1, a_2, \ldots)$, atunci a_i se numește *coeficientul de rang i* al polinomului f. Evident $f = g$ dacă și numai dacă coeficientul de rang i al lui f este egal cu coeficientul de rang i al lui g, oricare ar fi $i = 0, 1, 2, \ldots$. Șirul (0,0,0,...) poartă numele de *polinomul zero*. Operațiile inelului B se numesc respectiv *adunarea* și *înmulțirea* polinoamelor.

Fie $f \in B$, $f = (a_0, a_1, a_2, \ldots)$, $f \neq (0, 0, 0, \ldots)$. Cum numărul coeficienților diferiți de 0 ai lui f este finit, există un rang m astfel încît $a_m \neq 0$ și $a_i = 0$, oricare ar fi $i > m$. Atunci:

$$f = (a_0, a_1, \ldots, a_m, 0, \ldots), \qquad a_m \neq 0.$$

Numărul $m \in \mathbf{N}$ astfel determinat se numește *gradul* polinomului f, notat cu grad f, iar a_m se numește coeficientul *dominant* al lui f. Prin definiție, polinomul zero are gradul $-\infty$.

2. **Forma algebrică a polinoamelor.** Fie B inelul polinoamelor cu coeficienți în A construit mai sus. Deocamdată sîntem departe de ceea ce s-a înțeles prin polinoame în clasele anterioare. Vom obține scrierea uzuală a polinoamelor *(forma algebrică)* printr-o serie de identificări și convenții de notații.

De la inelul A la inelul de polinoame B considerăm aplicația

$$\varphi : A \to B, \ \varphi(a) = (a, 0, 0, \ldots), \qquad \forall a \in A.$$

Aplicația φ este injectivă căci dacă $\varphi(a) = \varphi(a')$, atunci $(a, 0, 0, \ldots) = (a', 0, 0, \ldots)$, deci $a = a'$. Pentru orice $a, b \in A$, avem:

$$\varphi(a + b) = (a + b, 0, 0, \ldots) = (a, 0, 0, \ldots) + (b, 0, 0, \ldots) = \\ = \varphi(a) + \varphi(b)$$

și

$$\varphi(ab) = (ab, 0, 0, \ldots) = (a, 0, 0, \ldots)(b, 0, 0, \ldots) = \varphi(a)\varphi(b).$$

Așadar, φ pune în corespondență biunivocă elementele lui A cu polinoamele de grad $\leqslant 0$.

Făcînd identificarea

$$a \equiv (a, 0, 0, \ldots), \ \forall a \in A$$

avem $A \subset B$ iar adunarea și înmulțirea elementelor lui A coincide cu adunarea și înmulțirea polinoamelor de grad $\leqslant 0$.

Considerăm polinomul $X = (0, 1, 0, \ldots)$. Conform regulii de înmulțire a polinoamelor se obține:

$$X^2 = XX = (0, 0, 1, 0, \ldots)$$
$$X^3 = X^2 X = (0, 0, 0, 1, 0, \ldots)$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$X^i = X^{i-1} X = (\underbrace{0, 0, \ldots, 0}_{i \text{ ori}}, 1, 0, \ldots)$$
$$\ldots\ldots\ldots\ldots\ldots$$

Pentru orice $a \in A$, avem:

$$aX^i \overset{\text{def}}{=} (a, 0, 0, \ldots)X^i = (\underbrace{0, 0, \ldots, 0}_{i \text{ ori}}, a, 0, \ldots).$$

Fie acum un polinom f de grad m, $f = (a_0, a_1, \ldots, a_m, 0, \ldots)$, $a_m \neq 0$. Avem: $f = (a_0, a_1, \ldots, a_m, 0, \ldots) = (a_0, 0, 0, \ldots) + (0, a_1, 0, \ldots) + \ldots + (0, 0, 0, \ldots, a_m, 0, \ldots) = a_0 + a_1 X + \ldots + a_m X^m$, deci

$$f = a_0 + a_1 X + \ldots + a_m X^m \qquad a_m \neq 0$$

numită *forma algebrică* a polinomului f. Dacă $a_m = 1$ spunem că polinomul f este *unitar*.

Inelul B va fi notat în continuare cu $A[X]$ și se numește *inelul polinoamelor în nedeterminata X cu coeficienți din A*.

Așadar, cu $\mathbf{Z}[X]$, $\mathbf{Z}_n[X]$, $\mathbf{Q}[X]$, $\mathbf{R}[X]$, $\mathbf{C}[X]$, $\mathbf{Z}_p[X]$, vom nota inelul polinoamelor în nedeterminata X cu coeficienții respectiv din $\mathbf{Z}$, $\mathbf{Z}_n$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Z}_p$.

Fie $f, g \in A[X]$, $f = a_0 + a_1 X + \ldots + a_m X^m$, $g = b_0 + b_1 X + \ldots + b_n X^n$ cu $a_m \neq 0$, $b_n \neq 0$. Pentru a face o alegere, presupunem $m \leqslant n$. Atunci:

$$f + g = a_0 + a_1 X + \ldots + a_m X^m + b_0 + b_1 X + \ldots + b_n X^n = \\ = (a_0 + b_0) + (a_1 + b_1)X + \ldots + (a_m + b_m)X^m + b_{m+1} X^{m+1} + \ldots + b_n X^n$$

și

$$fg = (a_0 + a_1X + \ldots + a_mX^m)(b_0 + b_1X + \ldots + b_nX^n) = a_0b_0 +$$
$$+ (a_0b_1 + a_1b_0)X + \ldots + (\sum_{i+j=k} a_ib_j)X^k + \ldots + a_mb_nx^{m+n}.$$

Din acest calcul se deduce:

$$\text{grad}\,(f+g) \leqslant \max\{\text{grad}\,f, \text{grad}\,g\}$$

și

$$\text{grad}(fg) \leqslant \text{grad}\ f + \text{grad}\ g.$$

Formulele de mai sus rămîn adevărate și atunci cînd $f = 0$ sau $g = 0$. Să observăm că în prima formulă avem inegalitate strictă dacă și numai dacă $m = n$ și $a_n = -b_n$.

Dacă $f \neq 0$ și $g \neq 0$ și inelul A este fără divizori ai lui zero, atunci $fg \neq 0$ căci din $a_m \neq 0$ și $b_n \neq 0$ se deduce $a_mb_n \neq 0$. Mai mult, în acest caz

$$\text{grad}\,(fg) = \text{grad}\ f + \text{grad}\ g.$$

Așadar:

1.1. *Teoremă.* **Dacă A este domeniu de integritate, atunci $A[X]$ este domeniu de integritate și**

$$\text{grad}\,(fg) = \text{grad}\ f + \text{grad}\ g, \qquad \forall f, g \in A[X],\ f \neq 0,\ g \neq 0.$$

3. **Funcții polinomiale. Rădăcini.** Fie A un inel comutativ, $f \in A[X]$, $f = a_0 + a_1X + \ldots + a_mX^m$ și $x \in A$. Elementul $f(x) \in A$,

$$f(x) \overset{\text{def}}{=} a_0 + a_1x + \ldots + a_mx^m$$

se numește *valoarea* polinomului f în punctul $x \in A$.

1.2. *Teoremă.* **Valoarea sumei (produsului) a două polinoame $f, g \in A[X]$ într-un punct $x \in A$ este egală cu suma (respectiv produsul) valorilor polinoamelor f și g în punctul x:**

$$(f+g)(x) = f(x) + g(x), \qquad \forall f, g \in A[X],\ x \in A$$
$$(fg)(x) = f(x)g(x), \qquad \forall f, g \in A[X],\ x \in A.$$

Demonstrație. Fie $f, g \in A[X]$, $f = a_0 + a_1X + a_2X^2 + \ldots$, $g = b_0 + b_1X + b_2X^2 + \ldots$ Atunci oricare ar fi $x \in A$ avem:

$$f(x) + g(x) = (a_0 + a_1x + a_2x^2 + \ldots) + (b_0 + b_1x + b_2x^2 + \ldots) =$$
$$= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots = (f+g)(x)$$

și

$$f(x)g(x) = (a_0 + a_1x + a_2x^2 + \ldots)(b_0 + b_1x + b_2x^2 + \ldots) =$$
$$= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \ldots = (fg)(x).$$

Fie $f \in A[X]$. Asociind la fiecare element $x \in A$ valoarea $f(x)$ a polinomului f în punctul x se obține o funcție $\tilde{f} : A \to A$,

$$\tilde{f}(x) = f(x), \qquad \forall x \in A,$$

numită *funcția polinomială* asociată lui f.

Dacă $f \in A[X]$, atunci zerourile funcției polinomiale asociate $\tilde{f} : A \to A$ se numesc *rădăcini* (din A) ale polinomului f. Cu alte cuvinte, un element $a \in A$ se numește *rădăcină* (din A) a polinomului $f \in A[X]$ dacă valoarea lui f în punctul a este egală cu zero, adică $f(a) = 0$. Determinarea rădăcinilor unui polinom dat este o problemă complexă. O serie de rezultate în legătură cu această problemă vor fi date în acest manual.

Exemple

1. Fie $f \in \mathbf{R}[X]$, $f = 7 - 6X + X^2$, atunci funcția polinomială asociată lui f este funcția reală de o variabilă reală $\tilde{f} : \mathbf{R} \to \mathbf{R}$,

$$\tilde{f}(x) = f(x) = 7 - 6x + x^2, \qquad \forall x \in \mathbf{R}.$$

Rădăcinile (din $\mathbf{R}$) ale polinomului f sînt

$$x_{1,2} = 3 \pm \sqrt{3^2 - 7} = 3 \pm \sqrt{2}.$$

Funcțiile polinomiale asociate polinoamelor cu coeficienți reali sînt studiate în Analiză.

2. Dacă $f, g \in \mathbf{Z}_3[X]$, $f = X^3 + \hat{2}X^2 + X + \hat{1}$, $g = \hat{2}X^2 + \hat{2}X + \hat{1}$ (coeficienții nespecificați sînt egali cu $\hat{1}$) atunci funcțiile polinomiale asociate $\tilde{f} : \mathbf{Z}_3 \to \mathbf{Z}_3$, $\tilde{g} : \mathbf{Z}_3 \to \mathbf{Z}_3$ pot fi descrise prin valorile lor în orice $x \in \mathbf{Z}_3$ folosind tabelele:

x	$\hat{0}$	$\hat{1}$	$\hat{2}$
$f(x)$	$\hat{1}$	$\hat{2}$	$\hat{1}$

x	$\hat{0}$	$\hat{1}$	$\hat{2}$
$g(x)$	$\hat{1}$	$\hat{2}$	$\hat{1}$

Se vede pe acest caz că $f \neq g$ și totuși $\tilde{f} = \tilde{g}$.

Să mai observăm că polinoamele f și g nu au rădăcini în $\mathbf{Z}_3$.

3. Polinomul $f = 2X - 7 \in \mathbf{Z}[X]$ nu are rădăcini în $\mathbf{Z}$. În adevăr, dacă pentru $a \in \mathbf{Z}$ avem $f(a) = 0$, atunci $2a - 7 = 0$, deci $2a = 7$. Dar $2a$ este par și 7 este impar. Contradicție.

4. Orice polinom f de grad 1 cu coeficienți dintr-un corp comutativ K admite o rădăcină în K. În adevăr, fie $f \in K[X]$, $f = a + bX$, unde $a, b \in K$, $b \neq 0$. Fie $c = -b^{-1}a \in K$. Atunci

$$f(c) = a + bc = a + b(-b^{-1}a) = a - bb^{-1}a = a - a = 0.$$

5. Rădăcinile în $\mathbf{Z}_5$ ale polinomului $f \in \mathbf{Z}_5[X]$, $f = X^2 + \hat{1}$ sînt $\hat{2}$ și $\hat{3}$. În adevăr, funcția polinomială asociată, $\tilde{f} : \mathbf{Z}_5 \to \mathbf{Z}_5$ ia valorile date în tabelul:

x	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$
$f(x)$	$\hat{1}$	$\hat{2}$	0	$\hat{0}$	$\hat{2}$

Rezultă că $f(\hat{2}) = \hat{0}$, $f(\hat{3}) = \hat{0}$. Polinomul $f \in \mathbf{R}[X]$, $f = X^2 + 1$ nu are nici o rădăcină în $\mathbf{R}$ căci dacă $f(a) = 0$ cu $a \in \mathbf{R}$, atunci $a^2 + 1 = 0$ deci $0 < a^2 = -1 < 0$. Contradicție.

Exerciții rezolvate

R — 1 Fie B inelul polinoamelor cu coeficienți în $\mathbf{Z}$ și $h \in B$, grad $h = 3$, $h = (-1, 6, -12, 8, 0, ...)$.

1) Să se determine polinoamele $f, g \in B$ astfel încît

$$h = fg, \text{ grad } f = 1, \text{ grad } g = 2.$$

2) Scrieți apoi polinoamele f, g, h sub forma algebrică și verificați că $fg = h$.

Soluție. 1) Cum grad $f = 1$ și grad $g = 2$, avem:

$$f = (a_0, a_1, 0, ...), \qquad g = (b_0, b_1, b_2, 0, ...)$$

cu $a_i, b_j \in \mathbf{Z}$, $a_1 \neq 0$, $b_2 \neq 0$. Conform definiției înmulțirii polinoamelor avem:

$$fg = (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1, a_1b_2, 0, ...)$$

și cum $fg = h$, din definiția egalității polinoamelor, rezultă:

$$\begin{cases} a_0b_0 = -1, \\ a_0b_1 + a_1b_0 = 6, \\ a_0b_2 + a_1b_1 = -12, \\ a_1b_2 = 8. \end{cases}$$

Dar din $a_0b_0 = -1$ cu $a_0, b_0 \in \mathbf{Z}$ rezultă că $a_0 = 1$, $b_0 = -1$ sau $a_0 = -1$, $b_0 = 1$. Cînd $a_0 = 1$, $b_0 = -1$, avem:

$$\begin{cases} b_1 - a_1 = 6, \\ b_2 + a_1b_1 = -12, \\ a_1b_2 = 8, \end{cases}$$

de unde $a_1 = -2$, $b_1 = 4$, $b_2 = -4$, deci

$$f = (1, -2, 0, ...), \qquad g = (-1, 4, -4, 0, ...).$$

Analog, cînd $a_0 = -1$, $b_0 = 1$ se găsește $f_1 = (-1, 2, 0, ...) = -f$ și $g_1 = (1, -4, 4, 0, ...) = -g$.

2) Avem:

$$f = (1, -2, 0, ...) = 1 - 2X,$$

$$g = (-1, 4, -4, 0, ...) = -1 + 4X - 4X^2,$$

$$h = (-1, 6, -12, 8, 0, ...) = -1 + 6X - 12X^2 + 8X^3.$$

Folosind proprietățile adunării și înmulțirii inelului $B = \mathbf{Z}[X]$, avem:

$$fg = (1 - 2X)(-1 + 4X - 4X^2) = (1 - 2X)(-1) + (1 - 2X) \cdot 4X +$$

$$+ (1 - 2X)(-4X^2) = -1 + 2X + 4X - 8X^2 - 4X^2 + 8X^3 = -1 + 6X - 12X^2 +$$

$$+ 8X^3 = h.$$

R — 2 Determinați toate polinoamele $f \in \mathbf{Z}_4[X]$ astfel încît

$$f^2 = \hat{0} \text{ și grad } f = 1.$$

Aceeași problemă pentru polinoamele inelului $\mathbf{Z}_5[X]$.

Soluție. Fie $f = \hat{a} + \hat{b}X \in \mathbf{Z}_4[X]$, $\hat{b} \neq \hat{0}$. Cum $f^2 = 0$ rezultă că

$$0 = f^2 = (\hat{a} + \hat{b}X)(\hat{a} + \hat{b}X) = \hat{a}^2 + 2\hat{a}\hat{b}X + \hat{b}^2X^2$$

și deci, prin identificarea coeficienților, avem:

$$(S) \begin{cases} \hat{a}^2 = \hat{0}, \\ 2\hat{a}\hat{b} = \hat{0}, \\ \hat{b}^2 = \hat{0}. \end{cases}$$

Dar $\mathbf{Z}_4 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}\}$ și $\hat{0}^2 = \hat{0}$, $\hat{1}^2 = \hat{1}$, $\hat{2}^2 = \hat{0}$, $\hat{3}^2 = \hat{1}$.

Rezultă că soluțiile sistemului (S) sînt $(\hat{0}, \hat{0})$, $(\hat{0}, \hat{2})$, $(\hat{2}, \hat{0})$ și $(\hat{2}, \hat{2})$. Cum $\hat{b} \neq \hat{0}$, deducem că polinoamele căutate sînt $\hat{2}X$ și $\hat{2} + \hat{2}X$.

Observăm că $\mathbf{Z}_5$ este corp, deci inelul $\mathbf{Z}_5[X]$ nu are divizori ai lui zero și atunci din $f^2 = \hat{0}$ rezultă $f = \hat{0}$.

R — 3 Fie $f, g \in \mathbf{Z}[X]$, $f \neq 0$, $g \neq 0$ și $h = fg$. Arătați că următoarele afirmații sînt echivalente:

a) Toți coeficienții polinomului h sînt pari.

b) Cel puțin unul din polinoamele f, g are toți coeficienții pari.

Soluție. Fie $f = a_0 + a_1X + ...$, $g = b_0 + b_1X + ...$, $h = c_0 + c_1X + ...$

a) $\Rightarrow$ b) Presupunem că nici f și nici g nu are toți coeficienții pari. Fie a_s coeficientul impar de rang minim al lui f, b_t coeficientul impar de rang minim al lui g și $k = s + t$. Atunci

$$(*) \qquad c_k = \sum_{i+j=k} a_ib_j = a_sb_t + \sum_{\substack{i+j=k \\ i \neq s,\ j \neq t}} a_ib_j.$$

Dacă $i + j = k$ unde $k = s + t$ și $i \neq s$, $j \neq t$ rezultă $i > s$ și $j < t$ sau $i < s$ și $j > t$. În ambele cazuri a_ib_j este par, și atunci din (*) rezultă că a_sb_t este par. Contradicție, căci a_s și b_t sînt impare, deci a_sb_t este impar.

b) $\Rightarrow$ a) Presupunem că f are toți coeficienții pari. Atunci numerele

$$c_k = a_0b_k + a_1b_{k-1} + ... + a_kb_0, \qquad k = 0, 1, ...$$

sînt pare.

§ 2. TEOREMA ÎMPĂRȚIRII CU REST

Fie K un corp comutativ. Vom studia proprietățile aritmetice ale inelului $K[X]$. Vom vedea că aritmetica inelului $K[X]$ este în esență aceeași cu a inelului $\mathbf{Z}$ al întregilor raționali. O serie de particularități vor fi date de

natura corpului K, după cum va rezulta considerînd cazurile $K = \mathbf{C}$, $K = \mathbf{R}$, $K = \mathbf{Q}$.

Este știut că un concept fundamental al aritmeticii inelului $\mathbf{Z}$ este cel de *divizibilitate*: dacă $a, b \in \mathbf{Z}$, spunem că b *divide* pe a, și scriem $b \mid a$, dacă există $q \in \mathbf{Z}$ astfel încît $a = bq$.

Un examen atent al modulului în care s-au obținut o serie de proprietăți aritmetice în $\mathbf{Z}$ evidențiază rolul decisiv avut de către teorema împărțirii cu rest: *oricare ar fi* $a, b \in \mathbf{Z}$, $b \neq 0$, *există* $q, r \in \mathbf{Z}$ *unic determinați astfel încît*:

$$a = bq + r, \qquad 0 \leqslant r < |b|.$$

Această teoremă se extinde la polinoame într-o nedeterminantă X cu coeficienți într-un corp comutativ K, după cum urmează:

2.1. *Teoremă* **(a împărțirii cu rest). Fie** K **un corp comutativ și** $f, g \in K[X]$, $g \neq 0$. **Există două polinoame** $q, r \in K[X]$, **unic determinate, astfel încît**

$$f = gq + r, \qquad \text{grad } r < \text{grad } g.$$

Demonstrație. Existența. Cînd grad $f <$ grad g, luăm $q = 0, r = f$ și avem $gq + r = g \cdot 0 + f = f$ cu grad $r <$ grad g. Rămîne să examinăm cazul grad $f \geqslant$ grad g. Fie $m =$ grad f, $n =$ grad g, $m \geqslant n$ și

$$f = a_m X^m + a_{m-1} X^{m-1} + \ldots + a_1 X + a_0$$
$$g = b_n X^n + b_{n-1} X^{n-1} + \ldots + b_1 X + b_0,$$
$$a_m \neq 0, \; b_n \neq 0.$$

Cum $b_n \neq 0$ și K este corp, polinomul

$$a_m b_n^{-1} X^{m-n} g = a_m X^m + a_m b_n^{-1} b_{n-1} X^{m-1} + \ldots$$

are coeficienții în K. Atunci polinomul f_1,

$$f_1 = f - a_m b_n^{-1} X^{m-n} g = (a_{m-1} - a_m b_n^{-1} b_{n-1}) X^{m-1} + \ldots \qquad (*)$$

este din $K[X]$ și grad $f_1 \leqslant m - 1$ (avem grad $f_1 = m - 1$ dacă și numai dacă $a_{m-1} - a_m b_n^{-1} b_{n-1} \neq 0$). Presupunînd afirmația adevărată pentru polinoame f de grad $< m$, atunci pentru cuplul de polinoame f_1, g există $q_1, r_1 \in K[X]$ astfel încît

$$f_1 = gq_1 + r_1, \qquad \text{grad } r_1 < \text{grad } g. \qquad (**)$$

Din (*) și (**) rezultă că

$$f = g(q_1 + a_m b_n^{-1} X^{m-n}) + r_1$$

și afirmația este adevărată luînd $q = q_1 + a_m b_n^{-1} X^{m-n}$, $r = r_1$.

Unicitatea. Fie $q, q_0, r, r_0 \in K[X]$ astfel încît $f = gq + r = gq_0 + r_0$, grad $r <$ grad g, grad $r_0 <$ grad g. Rezultă că $g(q - q_0) = r_0 - r$. Dacă $r \neq r_0$, atunci $q - q_0 \neq 0$ și avem:

$n >$ grad $(r_0 - r) =$ grad $g(q - q_0) =$ grad $g +$ grad $(q - q_0) \geqslant$ grad $g = n$. Contradicție. Deci $r = r_0$. Atunci $g(q - q_0) = 0$ și cum $g \neq 0$, deducem $q - q_0 = 0$, deci $q = q_0$ (inelul $K[X]$ nu are divizori ai lui zero).

Polinoamele q, r din identitatea $f = gq + r$, grad $r <$ grad g, se numesc respectiv *cîtul* și *restul* împărțirii lui f prin $g \neq 0$.

Fie $f, g \in K[X]$. Vom spune că polinomul g *divide* polinomul f, și scriem $g \mid f$, dacă există un polinom $q \in K[X]$ astfel încît $f = gq$. Se mai spune că g este *divizor* sau *factor* al lui f în inelul $K[X]$. Este clar că polinomul g divide polinomul f dacă și numai dacă restul împărțirii lui f prin g este egal cu polinomul zero.

Exemple

1. Fie $f, g \in \mathbf{Q}[X]$, $f = 2X^5 + 9X^4 + 2X^3 - 17X^2 + 3X - 8$, $g = X^2 + 2X - 3$. Să aflăm cîtul și restul împărțirii lui f prin g. Cunoscutul algoritm al împărțirii ca rest al polinoamelor constă în repetarea de un număr finit de ori a calculului prescris la (*) din demonstrația teoremei precedente, $a_m b_n^{-1} X^{m-n}$ intrînd ca termen al cîtului la fiecare execuție a pasului (*). În cazul nostru $n = 2$ și $b_n = b_2 = 1$. Folosind organizarea uzuală a calculelor, avem:

$$\begin{array}{l|l} 2X^5 + 9X^4 + 2X^3 - 17X^2 + 3X - 8 & X^2 + 2X - 3 \\ \hline 2X^5 + 4X^4 - 6X^3 & 2X^3 + 5X^2 - 2X + 2 \\ \hline / \quad 5X^4 + 8X^3 - 17X^2 - 3X - 8 & \\ \quad 5X^4 + 10X^3 - 15X^2 & \\ \hline \quad / \quad -2X^3 - 2X^2 + 3X - 8 & \\ \quad -2X^3 - 4X^2 + 6X & \\ \hline \quad\quad / \quad 2X^2 - 3X - 8 & \\ \quad\quad 2X^2 + 4X - 6 & \\ \hline \quad\quad\quad / \quad -7X - 2 & \end{array}$$

Așadar, $q = 2X^3 + 5X^2 - 2X + 2$, $r = -7X - 2$ și avem:

$$gq + r = (X^2 + 2X - 3)(2X^3 + 5X^2 - 2X + 2) - 7X - 2 = 2X^5 + 9X^4 + 2X^3 - 17X^2 + 3X - 8 = f, \text{ grad } r = 1 < 2 = \text{grad } g.$$

2. Fie $f, g \in \mathbf{Z}_5[X]$, $f = \hat{2}X^3 + X^2 + \hat{3}X + \hat{2}$, $g = \hat{3}X + \hat{2}$.
Să aflăm cîtul și restul împărțirii lui f prin g. Folosind tablele adunării și înmulțirii claselor de resturi modulo 5, avem:

$$\begin{array}{l|l} \hat{2}X^3 + X^2 + \hat{3}X + \hat{2} & \hat{3}X + \hat{2} \\ \hline 2X^3 + 3X^2 & \hat{4}X^2 + X + \hat{2} \\ \hline / \quad \hat{3}X^2 + \hat{3}X + \hat{2} & \\ \quad \hat{3}X^2 + \hat{2}X & \\ \hline \quad / \quad X + \hat{2} & \\ \quad\quad X + \hat{4} & \\ \hline \quad\quad / \quad \hat{3} & \end{array}$$

Rezultă că $q = \hat{4}X^2 + X + \hat{2}$, $r = \hat{3}$ și avem:

$$gq + r = (\hat{3}X + \hat{2})(\hat{4}X^2 + X + \hat{2}) + \hat{3} = \hat{2}X^3 + X^2 + \hat{3}X + \hat{2} = f,$$

grad $r = 0 < 1 =$ grad g.

3. Să se determine numerele raționale α și β astfel încît polinomul $g = X^2 + 2X - 3$ să dividă polinomul $f = 2X^5 + 9X^4 + 2X^3 - 17X^2 + \alpha X + \beta$. Folosind algoritmul împărțirii cu rest se găsește că restul împărțirii lui f prin g este polinomul $r = (\alpha - 10)X + \beta + 6$. Punînd condiția ca $r = 0$, deducem $\alpha = 10$, $\beta = -6$.

§ 3. DIVIZORI DE GRAD 1

1. **Teorema lui Bézout.** Teorema împărțirii cu rest are o serie de consecințe importante privind împărțirea prin polinoame de grad 1.

3.1. *Teoremă (a restului).* **Fie K un corp comutativ, $f \in K[X]$ și $a \in K$. Atunci există un polinom $q \in K[X]$ unic determinat astfel încît**

$$f = (X - a)q + f(a).$$

Demonstrație. Conform Teoremei 2.1, există două polinoame q, $r \in K[X]$, unic determinate, astfel încît

$$f = (X - a)q + r, \qquad \text{grad } r < \text{grad}(X - a) = 1.$$

Cum gradul polinomului r este mai mic ca 1 rezultă că $r \in K$ și avem:

$$f(a) = ((X - a)q + r)(a) = (a - a)q(a) + r(a) = r(a) = r,$$

deci

$$f = (X - a)q + f(a).$$

Următorul rezultat, cunoscut și sub numele de *teorema Bézout*, stabilește o legătură dintre divizorii de grad 1 ai unui polinom $f \in K[X]$ și rădăcinile lui f din K.

3.2. *Consecință (teorema factorului).* **Fie $f \in K[X]$ și $a \in K$. Atunci polinomul $X - a$ divide polinomul f dacă și numai dacă $f(a) = 0$.**

Un alt rezultat important este următorul:

3.3. *Consecință.* **Fie K un corp comutativ și $f \in K[X]$.**

1) Dacă $a_1, a_2, \ldots, a_r$ sînt rădăcini distincte din K ale polinomului f, atunci $r \leqslant$ grad f și polinomul $(X - a_1)(X - a_2)\ldots(X - a_r)$ divide pe f.

2) Polinomul f are cel mult m rădăcini distincte în corpul K, unde $m =$ grad f.

Demonstrație. 1) Dacă $a_1, a_2, \ldots, a_r$ sînt rădăcini distincte din K ale lui f, atunci polinomul $\prod_{i=1}^{r}(X - a_i)$, divide pe f. În adevăr, cînd $r = 1$ afirmația

rezultă din Consecința 9.3. Fie $r > 1$ și presupunem că afirmația este adevărată pentru $r - 1$. Atunci există $g \in K[X]$ astfel încît

$$f = \left(\prod_{i=1}^{r-1}(X - a_i)\right)g.$$

Avem:

$$0 = f(a_r) = \left(\prod_{i=1}^{r-1}(a_r - a_i)\right)g(a_r)$$

și cum $a_r - a_i \neq 0$, $1 \leqslant i \leqslant r - 1$, rezultă că $g(a_r) = 0$. Aplicînd din nou Consecința 9.3, există $h \in K[X]$ astfel încît $g = (X - a_r)h$, de unde

$$f = \left(\prod_{i=1}^{r-1}(X - a_i)\right)g = \left(\prod_{i=1}^{r-1}(X - a_i)\right)(X - a_r)h = \left(\prod_{i=1}^{r}(X - a_i)\right)h.$$

2) Presupunem acum că $a_1, a_2, \ldots, a_r$ reprezintă mulțimea tuturor rădăcinilor distincte din K ale lui f, deducem

$$m = \text{grad } f = \text{grad}\left(\prod_{i=1}^{r}(X - a_i)\right) + \text{grad } h = r + \text{grad } h \geqslant r.$$

2. Schema lui Horner. Fie $f \in K[X]$, $f = a_mX^m + a_{m-1}X^{m-1} + \ldots + a_1X + a_0$, $a_m \neq 0$ și $a \in K$. Împărțind cu rest polinomul f prin polinomul $X - a$ se obține un cît $q = c_{m-1}X^{m-1} + \ldots + c_1X + c_0$, $c_{m-1} = a_m \neq 0$ și un rest $r = f(a) \in K$. Avem identitatea

$$f = q(X - a) + r,$$

deci

$$a_mX^m + a_{m-1}X^{m-1} + \ldots + a_1X + a_0 = (c_{m-1}X^{m-1} + c_{m-2}X^{m-2} + \ldots + c_1X + c_0)(X - a) + r$$

de unde

$$a_mX^m + a_{m-1}X^{m-1} + \ldots + a_1X + a_0 = c_{m-1}X^m + (c_{m-2} - ac_{m-1})X^{m-1} + \ldots + (c_0 - ac_1)X + r - ac_0.$$

Identificînd coeficienții, găsim formulele ce ne permit determinarea succesivă a coeficienților $c_{m-1}, c_{m-2}, \ldots, c_1, c_0$ ai polinomului q precum și valoarea r a restului, anume:

$$\begin{aligned} c_{m-1} &= a_m, \\ c_{m-2} &= ac_{m-1} + a_{m-2}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ c_0 &= ac_1 + a_1, \\ r &= ac_0 + a_0. \end{aligned}$$

Calculele se sistematizează cu ajutorul unui tabel cu două linii. În prima linie sînt trecuți coeficienții lui f în ordinea $a_m, a_{m-1}, \ldots, a_1, a_0$ și în a doua linie se trec succesiv, pe măsură ce sînt determinați cu formulele de mai sus, coeficienții cîtului $c_{m-1}, c_{m-2}, \ldots, c_1, c_0$ și restul r.

$$\begin{array}{c|cccc|c} a_m & a_{m-1} & \ldots & a_1 & a_0 & \\ \hline c_{m-1} & c_{m-2} & \ldots & c_0 & r & a \end{array}$$

Se observă că pentru a determina c_i, $i \neq m-1$, se înmulțește cu a coeficientul c_{i+1} (deja determinat) din stînga lui c_i și se adună rezultatul cu a_{i+1} care stă deasupra lui c_i. Analog se calculează r. Această organizare a calculelor este cunoscută sub numele de *schema lui Horner*.

Exemple

1. Fie $f \in \mathbf{Q}[X]$, $f = 2X^4 - 2X^3 - 15X^2 + 10X + 3$. Să determinăm cîtul și restul împărțirii lui f prin polinomul $X - 3$. Folosind schema lui Horner avem:

	2	−2	−15	10	3
3	2	4	−3	1	6 | 3

de unde rezultă că $q = 2X^3 + 4X^2 - 3X + 1$ și $r = 6 = f(3)$.

2. Fie $f \in \mathbf{Z}_5[X]$, $f = X^3 + \hat{3}X + \hat{4}$. Să aflăm cîtul și restul împărțirii lui f prin polinomul $\hat{X} + \hat{3}$. Avem $X + \hat{3} = X - \hat{2}$ și folosind schema lui Horner,

	$\hat{1}$	$\hat{0}$	$\hat{3}$	$\hat{4}$
$\hat{2}$	$\hat{1}$	$\hat{2}$	$\hat{2}$	$\hat{3}$ | $\hat{2}$

deducem că $q = X^2 + \hat{2}X + \hat{2}$ și $r = \hat{3} = f(\hat{2})$.

Exerciții rezolvate

R—1 Fie $f \in \mathbf{R}[X]$, $f = X^3 - 9X^2 + 25X - 17$. Folosind schema lui Horner, determinați $r_0, r_1, r_2 \in \mathbf{R}$ astfel încît

$$f = (X-2)^3 + r_2(X-2)^2 + r_1(X-2) + r_0$$

(numită *dezvoltarea polinomului f după puterile lui $(X-2)$*).

Soluție. Putem scrie succesiv

$f = (X-2)q_0 + r_0$, unde $q_0 = (X-2)^2 + r_2(X-2) + r_1$,
$q_0 = (X-2)q_1 + r_1$, unde $q_1 = (X-2) + r_2$,
$q_1 = (X-2)q_2 + r_2$, unde $q_2 = 1$

deci
$r_0 = f(2)$, $r_1 = q_0(2)$, $r_2 = q_1(2)$. Așadar, ca să găsim r_0, r_1 și r_2 este necesar să determinăm polinoamele q_0 și q_1 și apoi valorile $f(2)$, $q_0(2)$ și $q_1(2)$ ceea ce se poate realiza prin folosirea de trei ori a schemei lui Horner. Calculele se pot organiza astfel

	1	−9	25	−17 |
2	1	−7	11	5	2
2	1	−5	1	2	
	1	−3	2		

	f		
	q_0	r_0	2
	q_1	r_1	2
	q_2	r_2	2

Deducem că $r_0 = 5$, $r_1 = 1$, $r_2 = -3$, de unde

$$f = (X-2)^3 - 3(X-2)^2 + (X-2) + 5.$$

R—2 Fie K un corp comutativ, $f \in K(X)$ și $a, b \in K$ cu $a \neq b$.

1) Arătați că restul împărțirii polinomului f prin polinomul $(X-a)(X-b)$ este

$$\frac{f(a)-f(b)}{a-b}X + \frac{af(b)-bf(a)}{a-b}.$$

2) Deduceți că dacă $X-a$ și $X-b$ divid pe f și $a \neq b$, atunci $(X-a)(X-b)$ divide pe f.

3) Arătați că polinomul $f = X^4 + X^3 - X^2 - 2X - 2 \in \mathbf{R}[X]$ se divide prin $X^2 - 2$.

Soluție. 1) Cum polinomul $g = (X-a)(X-b)$ este de grad 2 restul împărțirii lui f prin g este de forma $cX + d$, cu $c, d \in K$. Există $q \in K[X]$ astfel încît

$$f = (X-a)(X-b)q + cX + d,$$

de unde $f(a) = ca + d$ și $f(b) = cb + d$. Cum $a \neq b$, deducem că

$$c = \frac{f(a)-f(b)}{a-b}, \qquad d = \frac{af(b)-bf(a)}{a-b}.$$

2) Dacă $X-a \mid f$ și $X-b \mid f$, atunci $f(a) = f(b) = 0$, de unde

$$f = (X-a)(X-b)q.$$

3) Cum $X^2 - 2 = (X-\sqrt{2})(X+\sqrt{2})$ și $\sqrt{2} \neq -\sqrt{2}$, este suficient să arătăm că $X-\sqrt{2} \mid f$ și $X+\sqrt{2} \mid f$.
În adevăr, $f(\sqrt{2}) = 0$ și $f(-\sqrt{2}) = 0$, ceea ce se poate verifica cu schema lui Horner.

	1	-1	-2	-2 |
$\sqrt{2}$	1	$1+\sqrt{2}$	$1+\sqrt{2}$	$\sqrt{2}$ | 0
$-\sqrt{2}$	1	$1-\sqrt{2}$	$1-\sqrt{2}$	$-\sqrt{2}$ | 0

§ 4. RELAȚIA DE DIVIZIBILITATE PENTRU POLINOAME CU COEFICIENȚI ÎNTR-UN CORP

Fie K un corp comutativ și $f, g \in K[X]$. Am spus că polinomul g *divide* polinomul f dacă există un polinom $q \in K[X]$ astfel încît $f = gq$. În acest caz scriem $g \mid f$ și se mai spune că g este *divizor (factor)* al lui f în inelul $K[X]$ sau că f este *multiplu* al lui g în inelul $K[X]$.

i) *Relația de divizibilitate este reflexivă*: $f \mid f$, $\forall f \in K[X]$.
În adevăr, pentru orice $f \in K[X]$ avem $f = fg$ cu $q = 1 \in K[X]$.

ii) *Relația de divizibilitate este tranzitivă*: dacă $f \mid g$ și $g \mid h$, *atunci* $f \mid h$.

În adevăr, dacă $f \mid g$ și $g \mid h$, atunci există $q_1, q_2 \in K[X]$ astfel încît $g = fq_1$ și $h = gq_2$. Atunci

$$h = gq_2 = (fq_1)q_2 = f(q_1q_2) = fq$$

cu $q = q_1q_2 \in K[X]$, deci $g \mid h$.

iii) Dacă $h \mid f$ și $h \mid g$, atunci $h \mid uf + vg$, *oricare ar fi* $u, v \in K[X]$.

În adevăr, există $q_1, q_2 \in K[X]$ astfel încît $f = hq_1$ și $g = hq_2$. Atunci

$$uf + vg = uhq_1 + vhq_2 = h(uq_1 + vq_2) = hq,$$

cu $q = uq_1 + vq_2 \in K[X]$, deci $h \mid uf + vg$.

iv) Dacă $g \mid f$ și $f \neq 0$, *atunci* $0 \leqslant \text{grad } g \leqslant \text{grad } f$.

În adevăr, fie $q \in K[X]$ astfel încît $f = gq$. Atunci $g \neq 0$, $q \neq 0$ și deci

$$0 \leqslant \text{grad } g \leqslant \text{grad } g + \text{grad } q = \text{grad } f.$$

v) *Dacă* f, g *sînt două polinoame unitare din* $K[X]$ *astfel încît* $g \mid f$ și grad f = grad g, *atunci* $f = g$.

În adevăr, fie $f = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$, $g = X^n + b_{n-1}X^{n-1} + \ldots + b_1X + b_0$. Cum $g \mid f$, există $q \in K[X]$ astfel încît $f = gq$. Dar

$$n = \text{grad } f = \text{grad } g + \text{grad } q = n + \text{grad } q$$

deci grad $q = 0$, de unde $q = a \in K$, $a \neq 0$. Așadar, $f = ag$, deci

$$X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 = aX^n + ab_{n-1}X^{n-1} + \ldots + ab_1X + ab_0.$$

Identificînd coeficienții găsim $a = 1$ și $a_i = ab_i = b_i$, $0 \leqslant i \leqslant n-1$, deci $f = g$.

vi) *Dacă* $f, g \in K[X]$ *și* $g \mid f$, *atunci* $ag \mid f$, $a \in K$, $a \neq 0$. În adevăr, fie $q \in K[X]$ astfel încît $f = gq$. Dacă $a \in K$, $a \neq 0$, atunci $a^{-1} \in K$, deci $a^{-1}q$ este un polinom cu coeficienți în K și cum $f = (ag)(a^{-1}q)$, rezultă că $ag \mid f$.

4.1. *Definiție.* Fie $f, g \in K[X]$. Spunem că **polinomul** f **este** *asociat în divizibilitate* **cu** g, **și scriem** $f \sim g$, **dacă** $f \mid g$ **și** $g \mid f$.

4.2. *Teoremă.* Fie $f \in K[X]$, $f = a_mX^m + \ldots + a_1X + a_0$, $a_m \neq 0$.

1) **Un polinom** $g \in K[X]$ **este asociat în divizibilitate cu polinomul** f **dacă și numai dacă există** $a \in K$, $a \neq 0$, **astfel încît** $g = af$.

2) **Polinomul** $f^* = a_m^{-1}f = X^m + a_m^{-1}a_{m-1}X^{m-1} + \ldots + a_m^{-1}a_0$ **este singurul polinom unitar din** $K[X]$ **asociat în divizibilitate cu polinomul** f.

Demonstrație. 1) Presupunem că $g = af$, $a \neq 0$. Atunci avem $f \mid g$. Cum $f = bg$, unde $b = a^{-1} \in K$, avem și $g \mid f$, deci $f \sim g$.

Reciproc, dacă $f \sim g$, atunci $f \mid g$ și $g \mid f$, deci există $q_1, q_2 \in K[X]$ astfel încît $f = gq_1$ și $g = fq_2$. Deducem că $f = fq_1q_2$, deci $1 = q_1 \cdot q_2$.
Din relația $1 = q_1q_2$ rezultă că q_2 este polinom de grad zero, deci $q_2 = a \in K$, $a \neq 0$ și avem $g = af$.

2) Cum $f^* = a_m^{-1}f$ și $a_m^{-1} \in K$, $a_m^{-1} \neq 0$, rezultă că $f^* \sim f$.

Fie $h \in K[X]$ un polinom unitar astfel încît $h \mid f$. Cum $h \mid f$ și $f \mid f^*$ rezultă că $h \mid f^*$. Dar h și f^* fiind polinoame unitare și de același grad (= grad f), din $h \mid f^*$ rezultă $h = f^*$ (v. proprietatea v).

Exemple

1. Dacă $f \in \mathbb{Q}[X]$, $f = \frac{3}{5}X^2 - \frac{2}{3}X + \frac{3}{7}$, atunci polinomul unitar asociat în divizibilitate cu f este

$$f^* = \frac{5}{3}f = X^2 - \frac{10}{9}X + \frac{15}{21}.$$

Cum pentru orice $a \in \mathbb{Q}$, $a \neq 0$, polinomul af este asociat în divizibilitate cu f, rezultă că există o infinitate de polinoame în $\mathbb{Q}[X]$ asociate în divizibilitate cu f.

2. Fie $f \in \mathbb{Z}_5[X]$, $f = \hat{3}X^3 + \hat{2}X + \hat{4}$. Există doar patru polinoame asociate în divizibilitate cu f, anume

$$\hat{1}f = f = \hat{3}X^2 + \hat{2}X + \hat{4},$$
$$\hat{2}f = X^2 + \hat{4}X + \hat{3},$$
$$\hat{3}f = \hat{4}X^2 + X + \hat{2},$$
$$\hat{4}f = \hat{2}X^2 + \hat{3}X + \hat{1}.$$

§ 5. ALGORITMUL LUI EUCLID

Ca și în cazul numere întregi (v. Cap. I, § 4) se poate introduce noțiunea de c.m.m.d.c. pentru două polinoame cu coeficienți dintr-un corp comutativ K.

5.1. *Definitie.* Fie $f, g \in K[X]$. **Un polinom** $d \in K[X]$ **se numește** *cel mai mare divizor comun* **(c.m.m.d.c.) al lui** f **și** g **dacă:**

1) $d \mid f$, $d \mid g$;
2) $h \mid f$, $h \mid g \Rightarrow h \mid d$.

Dacă două polinoame $d_1, d_2 \in K[X]$ satisfac simultan 1) și 2), atunci $d_1 \sim d_2$. În adevăr, cum d_1 satisface 1) și d_2 satisface 2) rezultă că $d_1 \mid d_2$. Analog, $d_2 \mid d_1$, deci $d_1 \sim d_2$. Să mai observăm că dacă polinomul d satisface 1) și 2) atunci ad, cu $a \in K$, $a \neq 0$ satisface, de asemenea, 1) și 2). Cu alte cuvinte c.m.m.d.c., în caz de există, este unic determinat mai puțin o asociere în divizibilitate. Punînd condiția suplimentară ca d să fie polinomul unitar, atunci c.m.m.d.c. este chiar unic determinat (v. Teorema 4.2).

Vom nota cu (f, g) c.m.m.d.c. al polinoamelor f, g.

5.2. *Lemă.* **Fie f, g, q și r patru polinoame cu coeficienți în corpul K legate prin relația**

$$f = gq + r.$$

În acest caz, (f, g) există dacă și numai dacă (g, r) există și avem:

$$(f, g) = (g, r).$$

Demonstrație. Să presupunem că (f, g) există. Fie $d \in K[X]$, $d = (f, g)$. Cum $d \mid f$ și $d \mid g$ rezultă că d divide și polinomul $r = f - gq = 1 \cdot f + (-q)g$, deci:

$$1')\ d \mid g,\ d \mid r.$$

Dacă $h \mid g$ și $h \mid r$, atunci h divide și polinomul $f = gq + r$, deci $h \mid d$. Așadar:

$$2')\ h \mid g,\ h \mid r \Rightarrow h \mid d.$$

Din 1') și 2') rezultă că (g, r) există și $(g, r) = d$.

Reciproc, presupunem că (g, r) există și fie $d = (g, r)$. Avem $d \mid g$ și $d \mid r$ și cum $f = gq + r$, avem și $d \mid f$. Dacă $h \mid f$ și $h \mid g$, atunci h divide și polinomul $r = f - gq$. Cum $d = (g, r)$, din $h \mid f$ și $h \mid r$ rezultă $h \mid d$. Deci (f, g) există și avem $(f, g) = d$.

Sîntem pregătiți să dovedim că pentru orice două polinoame $f, g \in K[X]$ există (f, g). Dacă $f \mid g$ sau $g \mid f$ este clar că $(f, g) = f$, respectiv $(f, g) = g$, în particular, $(f, 0) = f$, $(0, g) = g$.

5.3. *Teoremă.* **Fie K un corp comutativ și $f, g \in K[X]$. Atunci (f, g) există. Mai mult, există $u, v \in K[X]$ astfel încît**

$$d = uf + vg,$$

unde $d = (f, g)$.

Demonstrație neconstructivă. Conform observațiilor făcute înaintea enunțului teoremei, putem presupune că $f \neq 0$ și $g \neq 0$. Fie $d = uf + vg$ un polinom de grad minim printre polinoamele diferite de 0 ce se reprezintă ca o combinație liniară de f și g cu coeficienți $u, v \in K[X]$. Evident, d satisface 2) din Definiția 5.1. Rămîne să arătăm că $d \mid f$ și $d \mid g$. Dacă d nu divide f, există q, $r \in K[X]$, $r \neq 0$, astfel încît

$$f = dq + r,\ \text{grad}\ r < \text{grad}\ d.$$

Avem:

$$0 \neq r = f - dq = f - (uf + vg)q = (1 - uq)f + (-vq)g.$$

Deci r este un polinom diferit de 0, care se scrie ca o combinație liniară de f și g și are gradul strict mai mic decît gradul lui d. Contradicție. Rămîne adevărat că $d \mid f$ și analog se arată că $d \mid g$. Deci d satisface și 1) din definiția 5.1, de unde $d = (f, g)$, $d = uf + vg$.

Demonstrație constructivă (algoritmul lui Euclid). Dacă $g \mid f$, atunci $(f, g) = g = 0 \cdot f + 1 \cdot g$. Presupunem deci că g nu divide pe f. Există q_0, $r_0 \in K[X]$ astfel încît

$$(0)\quad f = gq_0 + r_0,\ \text{grad}\ r_0 < \text{grad}\ g,\ r_0 \neq 0.$$

De asemenea, există $q_1, r_1 \in K[X]$ astfel încît

$$(1)\quad g = r_0q_1 + r_1,\ \text{grad}\ r_1 < \text{grad}\ r_0.$$

Dacă $r_1 \neq 0$, există $q_2, r_2 \in K[X]$ astfel încît

$$(2)\quad r_0 = r_1q_2 + r_2,\ \text{grad}\ r_2 < \text{grad}\ r_1.$$

Dacă $r_{i-1} \neq 0$, există $q_i, r_i \in K[X]$ astfel încît

$$(i)\quad r_{i-2} = r_{i-1}\,q_i + r_i,\ \text{grad}\ r_i < \text{grad}\ r_{i-1}$$

ș.a.m.d.

Cum

$\text{grad}\ g > \text{grad}\ r_0 > \text{grad}\ r_1 > \ldots > \text{grad}\ r_i \geqslant 0$,

există un rang n astfel încît $r_n \neq 0$ și $r_{n+1} = 0$,

deci

$$(n-1)\quad r_{n-3} = r_{n-2}q_{n-1} + r_{n-1},\ \text{grad}\ r_{n-1} < \text{grad}\ r_{n-2},\ r_{n-1} \neq 0,$$
$$(n)\quad r_{n-2} = r_{n-1}q_n + r_n,\ \text{grad}\ r_n < \text{grad}\ r_{n-1},\ r_n \neq 0,$$
$$(n+1)\quad r_{n-1} = r_nq_{n+1} + 0.$$

Cum $(r_n, 0)$ există și $(r_n, 0) = r_n$, folosind Lema 5.2 deducem succesiv existența pentru (r_{n-1}, r_n), (r_{n-2}, r_{n-1}), ..., (r_1, r_2), (r_0, r_1), (g, r_0) și (f, g). Mai mult

$$r_n = (r_n, 0) = (r_{n-1}, r_n) = (r_{n-2}, r_{n-1}) = \ldots = (r_1, r_2) = (r_0, r_1) = (g, r_0) = (f, g).$$

Ansamblul de împărțiri succesive cu rest (0), (1), ..., $(n + 1)$ se numește *algoritmul lui Euclid* pentru polinoamele f, g. Am demonstrat: *c.m.m.d.c. al polinoamelor f, g există și este egal cu ultimul rest $\neq 0$ din algoritmul lui Euclid pentru f și g.*

Din relația (n) se scoate r_n ca o combinație liniară de r_{n-2} și r_{n-1},

$$r_n = (-q_n)r_{n-1} + 1 \cdot r_{n-2}.$$

Înlocuind r_{n-1} cu valoarea sa dată de relația $(n - 1)$,

$$r_{n-1} = r_{n-3} - r_{n-2}q_{n-1},$$

se obține r_n ca o combinație liniară de r_{n-3} și r_{n-2}. Se folosesc apoi succesiv relațiile $(n - 2)$, $(n - 3)$, ..., (2), (1) și (0) pentru a se obține în final r_n ca o combinație liniară de f și g,

$$r_n = uf + vg.$$

5.4. *Observație.* Dacă există $u, v \in K[X]$ astfel încît $uf + vg = 1$, atunci $(f, g) = 1$. În adevăr, fie $d = (f, g)$. Cum $d \mid f$ și $d \mid g$, rezultă $d \mid uf + vg$, deci $d \mid 1$. Singurul polinom unitar care divide pe 1 este 1, deci $d = 1$.

Exemple.

1. Fie $f, g \in \mathbb{Q}[X]$, $f = 6X^7 - X^6 + 18X^5 - 4X^4 + 15X^3 - 3X^2 + 6X + 2$, $g = 2X^5 + X^4 + 6X^3 + 2X^2 + 4X$. Să găsim (f, g) cu algoritmul lui Euclid. Avem succesiv:

$f = gq_0 + r_0$ unde $q_0 = 3X^2 - 2X + 1$, $r_0 = X^4 + X^3 + 3X^2 + 2X + 2$.
$g = r_0q_1 + r_1$, unde $q_1 = 2X - 1$, $r_1 = X^3 + X^2 + 2X + 2$,
$r_0 = r_1q_2 + r_2$, unde $q_2 = X$, $r_2 = X^2 + 2$,
$r_1 = r_2q_3 + r_3$, unde $q_3 = X + 1$, $r_3 = 0$,

deci,

$$r_2 = (f, g) = X^2 + 2.$$

Avem:

$$X^2 + 2 = r_2 = r_0 - r_1q_2 = r_0 - (g - r_0q_1)q_2 = f - qg_0 - (g - (f - gq_0)q_1)q_2 = (1 + q_1q_2)f + (-q_0 - q_2 - q_0q_1q_2)g,$$

deci

$(f, g) = uf + vg$, unde $u = 2X^2 - X + 1$, $v = 6X^4 - 7X^3 + X^2 - 1$.

2. Fie $f, g \in Z_5[X]$, $f = X^5 + \hat{3}X^4 + \hat{3}X^3 + X^2 + \hat{3}X + \hat{4}$, $g = \hat{2}X^4 + \hat{3}X^3 + \hat{4}X^2 + \hat{2}X + \hat{4}$.

Aplicînd algoritmul lui Euclid, să găsim (f, g). Avem:

$f = gq_0 + r_0$, unde $q_0 = \hat{3}X + \hat{2}$, $r_0 = \hat{2}X^2 + \hat{2}X + \hat{1}$,
$g = r_0q_1 + r_1$, unde $q_1 = X^2 + \hat{3}X + \hat{1}$, $r_1 = \hat{2}X + \hat{3}$,
$r_0 = r_1q_2 + r_2$, unde $q_2 = X + \hat{2}$, $r_2 = 0$,

deci

$$(f, g) = r_1 = \hat{2}X + \hat{3}.$$

Cum

$$r_1 = g - r_0q_1 = g - (f - gq_0)q_1 = (-q_1)f + (1 + q_0q_1)g$$

rezultă:

$(f, g) = uf + vg$, unde $u = \hat{4}X^2 + \hat{2}X + \hat{4}$, $v = \hat{3}X^3 + X^2 + \hat{4}X + \hat{3}$.

§ 6. POLINOAME IREDUCTIBILE

Fie K un corp comutativ și $K[X]$ inelul polinoamelor în nedeterminata X cu coeficienți din K. Vom vedea că pentru aritmetica inelului $K[X]$ noțiunea de *polinom ireductibil* care se definește mai jos joacă un rol similar celei de număr prim pentru aritmetica inelului $\mathbb{Z}$.

6.1. *Definiție.* **Fie K un corp comutativ și $\pi \in K[X]$ un polinom de gradul $n > 0$. Spunem că π este *polinom ireductibil* peste K dacă nu există $f, g \in K[X]$ astfel încît**

$$\pi = fg, \quad \text{grad } f < n, \quad \text{grad } g < n.$$

În caz contrar, spunem că π este *polinom reductibil* peste K.

Să observăm că dacă $\pi = fg$, atunci pentru orice $a \in K$, $a \neq 0$, avem:

$$a\pi = (af)g, \quad \text{grad } (af) = \text{grad } f.$$

Rezultă că dacă π este ireductibil (reductibil) peste K, atunci polinomul $a\pi$ este ireductibil (resp. reductibil) peste K, oricare ar fi $a \in K$, $a \neq 0$. În fine, să observăm că un polinom $\pi \in K[X]$ de grad $n > 0$ este ireductibil (reductibil) peste K dacă și numai dacă nu admite (resp. admite) un divizor $f \in K[X]$ astfel încît

$$0 < \text{grad } f < n.$$

Exemple

1. *Orice polinom de grad 1 din $K[X]$ este ireductibil peste K.* În adevăr, un polinom $\pi = aX + b$, cu $a, b \in K$, $a \neq 0$, nu poate avea divizori de grad diferit de 0 și 1 (v. proprietatea iv)) § 4).
2. *Dacă un polinom $\pi \in K[X]$ de grad $n > 1$ este ireductibil peste K, atunci π nu admite rădăcini în K. Reciproc, dacă un polinom $\pi \in K[X]$ de grad 2 sau 3 nu admite rădăcini în K, atunci π este ireductibil peste K.*

În adevăr, dacă grad $\pi = n > 1$ și $a \in K$ este o rădăcină a lui π, atunci conform teoremei lui Bézout $X - a \mid \pi$, deci există $q \in K[X]$ astfel încît

$$\pi = (X - a)q.$$

Cum $X - a \in K[X]$, $q \in K[X]$ și grad $(X - a) = 1 < n$. grad $q = n - 1 < n$ rezultă că π este reductibil peste K.

Reciproc, presupunem că gradul lui π este 2 sau 3 și că π este reductibil peste K. În acest caz π admite un divizor $f \in K[X]$ de grad 1, $f = aX + b$, cu $a \neq 0$. Atunci polinomul π admite rădăcina $c = -a^{-1}b \in K$.

Astfel, polinomul $\pi = X^2 - 2 \in \mathbb{Q}[X]$ este ireductibil peste $\mathbb{Q}$. În adevăr, în caz contrar, există $a \in \mathbb{Q}$ astfel încît $0 = \pi(a) = a^2 - 2$, de unde $\sqrt{2} \in \mathbb{Q}$. Contradicție.

Polinomul $\pi = X^2 - 2$ este reductibil peste $\mathbb{R}$ căci avem

$$\pi = (X - \sqrt{2})(X + \sqrt{2})$$

și

$$X - \sqrt{2} \in \mathbb{R}[X], \quad X + \sqrt{2} \in \mathbb{R}[X].$$

Polinomul $\pi = X^3 + \hat{2}X^2 + X + \hat{1} \in \mathbb{Z}_3[X]$ este ireductibil peste corpul $\mathbb{Z}_3$ căci π nu are nici o rădăcină în $\mathbb{Z}_3$. În adevăr, $\pi(\hat{0}) = \hat{1} \neq \hat{0}$, $\pi(\hat{1}) = \hat{2} \neq \hat{0}$ și $\pi(\hat{2}) = \hat{1} \neq \hat{0}$.

Să observăm că dacă un polinom $f \in K[X]$ admite un divizor $g \in K[X]$ de grad n, $g = b_n X^n + \ldots$, atunci admite și un divizor unitar de grad n din $K[X]$, de exemplu polinomul $g^* = b_n^{-1} g = X^n + \ldots$ (v. proprietatea vi)), § 4).

6.2. *Lemă.* **Orice polinom $f \in K[X]$ de grad mai mare ca 0 admite un divizor ireductibil unitar.**

Demonstrație. Polinomul f admite divizori din $K[X]$ de grad mai mare ca 0, de exemplu pe f. Printre divizorii lui f din $K[X]$ de grad mai mare ca 0 considerăm unul de grad minim, fie acesta π. Înlocuind eventual pe π cu π^*, putem presupune că π este unitar. Polinomul π este ireductibil peste K. În adevăr, dacă π este reductibil există $h \in K[X]$ astfel încît $h \mid \pi$ și $0 < \text{grad } h < \text{grad } \pi$. Dar din $h \mid \pi$ și $\pi \mid f$ rezultă $h \mid f$ și cum $0 < \text{grad } h < \text{grad } \pi$, este contrazisă alegerea lui π. Rămîne adevărat că π este ireductibil peste K.

6.3. *Teoremă.* **Pentru un corp comutativ K următoarele afirmații sînt echivalente:**

1) **Orice polinom ireductibil peste K are gradul 1.**

2) **Orice polinom f cu coeficienți din K de grad mai mare ca 0 admite cel puțin o rădăcină din K.**

Demonstrație. 1) $\Rightarrow$ 2 Conform Lemei 6.2 polinomul f admite un divizor ireductibil unitar $\pi \in K[X]$. Din 1) rezultă că π, are gradul 1 și atunci π este de forma $X - a$, $a \in K$. Cum $X - a \mid f$, din teorema lui Bézout rezultă că $f(a) = 0$, $a \in K$.

2) $\Rightarrow$ 1). Fie π un polinom ireductibil peste K. Din 2) rezultă că există $a \in K$ astfel încît $\pi(a) = 0$. Conform teoremei lui Bézout polinomul $X - a$ divide pe π. Cum $X - a \in K[X]$ și π este polinom ireductibil peste K, rezultă că π are gradul egal cu 1.

Spunem că un corp K este *algebric închis* dacă orice polinom $f \in K[X]$ de grad > 0 admite cel puțin o rădăcină în K. Corpul $\mathbf{Q}$ nu este algebric închis căci polinomul $X^2 - 2$ este ireductibil peste $\mathbf{Q}$ și are gradul 2 (v. Teorema 6.3). Nici corpul $\mathbf{R}$ nu este algebric închis căci polinomul $X^2 + 1$ nu admite rădăcini în $\mathbf{R}$. În adevăr, dacă pentru $a \in \mathbf{R}$ avem $a^2 + 1 = 0$, atunci $a^2 = -1 < 0$, contradicție.

Corpul $\mathbf{C}$ al numerelor complexe este algebric închis, acest rezultat fiind cunoscut sub numele de *teorema fundamentală a algebrei*:

6.4. *Teoremă.* (d'Alembert-Gauss). **Orice polinom f cu coeficienți complecși de grad mai mare ca 0 admite cel puțin o rădăcină complexă.**

Nu se cunoaște o demonstrație elementară pentru această teoremă. O admitem fără demonstrație.

6.5. *Consecință.* **Orice polinom ireductibil peste $\mathbf{C}$ are gradul unu.**

Demonstrație. Rezultă din teoremele 6.4 și 6.3.

Fie $f \in \mathbf{R}[X]$, $f = a_m X^m + a_{m-1} X^{m-1} + \ldots + a_1 X + a_0$. **Cum $\mathbf{R} \subset \mathbf{C}$,** avem $f \in \mathbf{C}[X]$. Conform Teoremei 6.4 există $z \in \mathbf{C}$, $z = a + ib$, cu $a, b \in \mathbf{R}$, astfel încît $f(z) = 0$, deci

$$a_m z^m + a_{m-1} z^{m-1} + \ldots + a_1 z + a_0 = 0.$$

Fie $\bar{z} = a - ib$ *conjugatul numărului complex* z. Avem:

$$0 = \bar{0} = \overline{a_m z^m + a_{m-1} z^{m-1} + \ldots + a_1 z + a_0} = \overline{a_m z^m} + \overline{a_{m-1} z^{m-1}} + \ldots + \overline{a_1 z} + \overline{a_0} = a_m \bar{z}^m + a_{m-1} \bar{z}^{m-1} + \ldots + a_1 \bar{z} + a_0,$$

de unde $f(\bar{z}) = 0$. Am demonstrat:

6.6. *Teoremă.* **Dacă numărul complex z este rădăcină a polinomului f cu coeficienți reali, atunci și $\bar{z}$ este rădăcină a lui f.**

6.7. *Consecință.* **Singurele polinoame unitare ireductibile peste corpul $\mathbf{R}$ sînt:**

1) **Polinoamele $X - a$, $a \in \mathbf{R}$;**

2) *Polinoamele* $X^2 + bX + c$, $b, c \in \mathbf{R}$, $b^2 - 4c < 0$.

Demonstrație. Polinoamele $X - a$, $a \in \mathbf{R}$ avînd gradul 1 sînt ireductibile peste $\mathbf{R}$.

Fie acum π un polinom unitar de grad $n > 1$ ireductibil peste $\mathbf{R}$. Polinomul π nu admite rădăcini reale. În adevăr, dacă $\pi(a) = 0$, cu $a \in \mathbf{R}$, atunci $X - a \mid \pi$. Deci π admite divizorul $X - a \in \mathbf{R}[X]$ de grad $1 \neq 0, n$ și atunci π este reductibil peste $\mathbf{R}$. Cum $\pi \in \mathbf{R}[X]$ rezultă că $\pi \in \mathbf{C}[X]$ și conform Teoremei 6.4 există $z \in \mathbf{C}$, $z = u + iv$, $u, v \in \mathbf{R}$ astfel încît $\pi(z) = 0$. Cum π are coeficienții reali, din Consecința 6.6 rezultă că și $\pi(\bar{z}) = 0$. Din $\pi(z) = 0$ rezultă că $X - z \mid \pi$, deci există $g \in \mathbf{C}[X]$ astfel încît

$$\pi = (X - z)g$$

și atunci

$$0 = \pi(\bar{z}) = (\bar{z} - z)g(\bar{z}). \qquad (*)$$

Cum polinomul π nu admite rădăcini reale avem $v \neq 0$, deci $z \neq \bar{z}$ și atunci din (*) rezultă că $g(\bar{z}) = 0$. Așadar $X - \bar{z} \mid g$, deci există $h \in \mathbf{C}[X]$ astfel încît $g = (X - \bar{z})h$. Avem:

$$\pi = (X - z)g = (X - z)(X - \bar{z})h = (X^2 - 2uX + u^2 + v^2)h.$$

Polinomul $X^2 - 2uX + u^2 + v^2 \in \mathbf{R}[X]$ și divide pe π. Cum π și $X^2 - 2uX + u^2 + v^2$ au coeficienții reali, rezultă că $h \in \mathbf{R}[X]$. Avem $n = 2$, deci $\pi = X^2 - 2uX + u^2 + v^2$ căci dacă $n > 2$ rezultă că π este reductibil peste $\mathbf{R}$. Notînd $b = -2u$, $c = u^2 + v^2$, avem $b^2 - 4c = 4u^2 - 4u^2 - 4v^2 = -4v^2 < 0$.

§ 7. DESCOMPUNEREA POLINOAMELOR ÎN PRODUS DE FACTORI IREDUCTIBILI

Se știe că oricare ar fi numărul întreg $a > 1$ există numerele prime $p_i > 0$, $1 \leqslant i \leqslant n$, unic determinate astfel încît

$$a = p_1 p_2 \ldots p_n,$$

rezultat cunoscut sub numele de *teorema fundamentală a Aritmeticii*. Un rezultat asemănător este adevărat și pentru polinoame cu coeficienți într-un corp comutativ K, locul numerelor prime fiind luat de către polinoamele ireductibile.

7.1. *Teoremă.* **Fie K un corp comutativ și $f \in K[X]$, $f = aX^m + \ldots$, cu $a \neq 0$ și $m > 0$.**

Există polinoamele ireductibile unitare $\pi_1, \pi_2, \ldots, \pi_n$, unic determinate, astfel încît

$$f = a\pi_1\pi_2 \ldots \pi_n.$$

Faptul că orice polinom $f \in K[X]$ cu grad $f = m > 0$, admite o asemenea descompunere se demonstrează imediat prin inducție asupra lui m. În adevăr, $f = af^*$, unde $f^* = a^{-1}f = X^m + \ldots$. Dacă $m = 1$, atunci f este ireductibil peste K (v. Exp. 1, §6) și rezultatul din enunț este adevărat cu $n = 1$. Presupunem că $m > 1$ și că teorema este adevărată pentru polinoame de grad mai mic ca m. Dacă f este ireductibil, din nou rezultatul din enunț este adevărat cu $n = 1$. Altfel, există două polinoame unitare $g, h \in K[X]$ astfel încît

$$f^* = gh, \text{ grad } g < m, \text{ grad } h < m.$$

Conform ipotezei inducției, g și h sînt produse finite de polinoame ireductibile unitare și atunci $f^* = gh$ este produs finit de polinoame ireductibile unitare.

Demonstrația unicității se propune ca exercițiu (v. Ex. 78).

7.2. *Consecință.* **Pentru orice polinom cu coeficienți complecși $f = a_mX^m + a_{m-1}X^{m-1} + \ldots + a_1X + a_0$, $m > 0$, $a_m \neq 0$, există $z_1, z_2, \ldots, z_m \in \mathbf{C}$ unic determinați astfel încît**

$$f = a_m(X - z_1)(X - z_2)\ldots(X - z_m).$$

Demonstrație. Rezultă din Teorema 7.1 și Consecința 6.5.

7.3. *Consecință.* **Orice polinom $f = a_mX^m + \ldots + a_1X + a_0$, $a_m \neq 0$, $m > 0$, $a_m \neq 0$, cu coeficienți reali se descompune în mod unic sub forma**

$$f = a_m(X - \alpha_1)\ldots(X - \alpha_s)(X^2 + \beta_1X + \gamma_1)\ldots(X^2 + \beta_tX + \gamma_t)$$

unde $\alpha_i, \beta_j, \gamma_j \in \mathbf{R}$, $\beta_j^2 - 4\gamma_j < 0$, $1 \leqslant j \leqslant t$ și $s + 2t = m$.

Demonstrație. Rezultă din Teorema 7.1 și Consecința 6.7.

Exemple.

1. Să descompunem în factori ireductibili peste $\mathbf{Q}$, $\mathbf{R}$ și $\mathbf{C}$ polinomul $f = X^4 + X^3 - X^2 - 2X - 2$ știind că admite rădăcina $x = -1/2 + i\sqrt{3}/2$.

Polinomul f avînd coeficienții reali, admite și rădăcina $\bar{z} = -1/2 - i\sqrt{3}/2$ și deci f se divide prin polinomul $(X + z)(X - \bar{z}) = X^2 + X + 1$ (v. Ex. R—2, § 3). Împărțind pe f prin $X^2 + X + 1$ se găsește cîtul $X^2 - 2$, deci

$$f = (X^2 - 2)(X^2 + X + 1). \tag{1}$$

Cum discriminantul polinomului $X^2 + X + 1$ este $\Delta = 1^2 - 4 \cdot 1 = -3 < 0$ rezultă că $X^2 + X + 1$ este ireductibil peste $\mathbf{R}$ și cu atît mai mult peste $\mathbf{Q}$. Am observat mai înainte că $X^2 - 2$ este inductibil peste $\mathbf{Q}$. Deci (1) este descompunerea lui f în factori inductibili peste $\mathbf{Q}$. Descompunerile lui f în factori ireductibili peste $\mathbf{R}$ și $\mathbf{C}$ sînt:

$$f = (X - \sqrt{2})(X + \sqrt{2})(X^2 + X + 1)$$

respectiv

$$f = (X - \sqrt{2})(X + \sqrt{2})\left(X + \frac{1}{2} - \frac{i\sqrt{3}}{2}\right)\left(X + \frac{1}{2} + \frac{i\sqrt{3}}{2}\right).$$

2. Fie $f \in \mathbf{Z}_3[X]$, $f = X^3 + \hat{2}X^2 + X + \hat{2}$. Să descompunem pe f în factori ireductibili peste corpul $\mathbf{Z}_3$. Să observăm că un polinom de grad 2 sau 3 este reductibil peste corpul coeficienților dacă și numai dacă admite o rădăcină în corpul coeficienților. Valorile $f(x)$ ale polinomului f cînd $x \in \mathbf{Z}_3$ sînt:

x	$\hat{0}$	$\hat{1}$	$\hat{2}$
$f(x)$	$\hat{2}$	$\hat{0}$	$\hat{2}$

deci f se divide prin $X - \hat{1} = X + \hat{2}$. Folosind schema lui Horner, avem:

	$\hat{1}$	$\hat{2}$	$\hat{1}$	$\hat{2}$
$\hat{1}$		$\hat{1}$	$\hat{0}$	$\hat{1}$

deci cîtul lui f prin $X - \hat{1}$ este $X^2 + \hat{1}$, de unde:

$$f = (X - \hat{1})(X^2 + \hat{1}).$$

Polinomul $X^2 + \hat{1}$ nu are rădăcini în $\mathbf{Z}_3$, deci este ireductibil peste $\mathbf{Z}_3$. Descompunerea căutată este $f = (X - \hat{1})(X^2 + \hat{1})$.

§ 8. RĂDĂCINI MULTIPLE

În acest paragraf corpul K va fi unul din corpurile de numere $\mathbf{Q}$, $\mathbf{R}$ sau $\mathbf{C}$. Avem deci $K \subseteq C$ și atunci $K[X] \subseteq \mathbf{C}[X]$. În aceste condiții orice polinom f cu coeficienți în K poate fi considerat la nevoie ca fiind polinom cu coefi-

cienți din $\mathbf{C}$. O serie din rezultatele acestui paragraf rămîn adevărate și în cazul $K = \mathbf{Z}_p$, p număr prim.

Fie $f \in K[X]$ și $\alpha \in K$ o rădăcină a polinomului f. Cum $f(\alpha) = 0$, din teorema lui Bézout rezultă că $X - \alpha \mid f$. Se poate întîmpla să avem și $(X - \alpha)^2 \mid f$, $(X - \alpha)^3 \mid f$, ... Dacă $(X - \alpha)^h \mid f$, $h > 1$, atunci $h \leqslant \text{grad } f$, deci există $e \in N$, $e \geqslant 1$ astfel încît:

$X - \alpha \mid f$, $(X - \alpha)^2 \mid f$,..., $(X - \alpha)^e \mid f$ și $(X - \alpha)^{e+1}$ nu divide f. Astfel, dacă $f = (X - 2)^3(X^2 + 1) \in \mathbf{R}[X]$ și $\alpha = 2$, atunci $e = 3$.

8.1. *Definiție.* **Fie $f \in K[X]$ și $\alpha \in K$ o rădăcină a polinomului f. Spunem că *ordinul de multiplicitate* al rădăcinii α este e, dacă $(X - \alpha)^e \mid f$ și $(X - \alpha)^{e+1}$ nu divide pe f.**

Dacă $e = 1$ spunem că α este o rădăcină *simplă* a lui f iar dacă $e > 1$ spunem că α este rădăcină *multiplă* a lui f. Cînd $e = 2, 3, ...$, α se numește, respectiv rădăcina *dublă*, *triplă*, ...

Să luăm polinomul $f = X^4 - 3X^3 + X^2 + 4 \in \mathbf{Q}[X]$ și să observăm că $f(2) = 0$. Deci $\alpha = 2$ este rădăcină a polinomului f. Se pune problema determinării ordinului de multiplicitate al rădăcinii $\alpha = 2$ a polinomului f. Împărțind polinomul f prin $X - 2$ găsim $f = (X - 2)g$, unde $g = X^3 - X^2 - X - 2$. Cum $g(2) = 0$, rezultă că $X - 2 \mid g$ și găsim $g = (X - 2)h$, $h = X^2 + X + 1$, deci $f = (X - 2)^2 h$. Cum $h(2) = 7 \neq 0$, $X - 2$ nu divide pe h, deci $(X - 2)^3$ nu divide pe f. Rezultă că $\alpha = 2$ este rădăcină dublă a polinomului f.

Un instrument eficace de determinare a ordinului de multiplicitate pentru rădăcinile unui polinom este dat de conceptul de *derivată formală* a polinoamelor: dacă $f \in K[X]$, $f = a_m X^m + a_{m-1} X^{m-1} + ... + a_1 X + a_0$, atunci *derivata* (formală) a polinomului f, notată cu Df, este:

$$Df = m a_m X^{m-1} + (m - 1) a_{m-1} X^{m-2} + ... + 2a_2 X + a_1.$$

Cînd $K = \mathbf{R}$, funcția polinomială $\tilde{f} : \mathbf{R} \to \mathbf{R}$ $\tilde{f}(x) = f(x) = a_m x^m + a_{m-1} x^{m-1} + ... + a_1 x + a_0$, $\forall x \in \mathbf{R}$, are derivată în sensul acestui concept al Analizei și după cum este știut

$$\tilde{f}'(x) = m a_{m-1} x^{m-1} + (m - 1) a_{m-1} x^{m-2} + ... + a_1 = \tilde{Df}(x), \ \forall x \in \mathbf{R}.$$

Așadar, cînd $K = \mathbf{R}$, derivata formală Df a polinomului f este legată de derivata $\tilde{f}'$ a funcției polinomiale $\tilde{f}$ prin:

$$\boxed{\tilde{f}' = \tilde{Df}, \ \forall f \in \mathbf{R}[X]}$$

Ca și pentru derivata funcțiilor reale, avem proprietățile:

$$D(f + g) = Df + Dg, \ D(fg) = Df \cdot g + f \cdot Dg, \ \forall f, g \in K[X],$$

ceea ce se poate verifica direct cu definiția dată pentru derivata formală a polinoamelor.

Definim succesiv $D^1 f = Df$, $D^2 f = D(D^1 f)$, ..., $D^h f = D(D^{h-1} f)$, ..., $D^h f$ numindu-se derivata formală de *ordin* h a polinomului f. Dacă $f = X^4 - 3X^3 + X^2 + 4 \in \mathbf{Q}[X]$, atunci:

$$D^1 f = Df = 4X^3 - 9X^2 + 2X,$$
$$D^2 f = D(D^1 f) = 12X^2 - 18X + 2,$$
$$D^3 f = D(D^2 f) = 24X - 18,$$
$$D^4 f = D(D^3 f) = 24,$$
$$D^5 f = D(D^4 f) = 0.$$

8.2. *Teoremă.* **Fie $f \in K[X]$ și $\alpha \in K$. Atunci α este rădăcină simplă a lui f dacă și numai dacă $f(\alpha) = 0$ și $D(f(\alpha) \neq 0$.**

Demonstrație. Fie $\alpha \in K$ o rădăcină a polinomului f. Cum $f(\alpha) = 0$, din teorema lui Bézout rezultă că $f = (X - \alpha)g$, cu $g \in K[X]$. Evident, $(X - \alpha)^2$ nu divide f dacă și numai dacă $X - \alpha$ nu divide g. Deci α este rădăcină sinplă a lui f dacă și numai dacă $g(\alpha) \neq 0$.

Pe de altă parte, avem:

$$Df = D((X - \alpha)g) = D(X - \alpha) \cdot g + (X - \alpha) Dg = g + (X - g) Dg,$$

de unde

$$Df(\alpha) = g(\alpha) + (\alpha - \alpha) Dg(\alpha) = g(\alpha).$$

Rezultă că α este rădăcină simplă a lui f dacă și numai dacă $f(\alpha) = 0$ și $Df(\alpha) \neq 0$.

8.3. *Consecință.* **Fie $f \in K[X]$ și $\alpha \in K$ o rădăcină a lui f. Atunci α este rădăcină multiplă a lui f dacă și numai dacă $Df(\alpha) = 0$.**

8.4. *Teoremă.* **Fie $f \in K[X]$ și $\alpha \in K$ o rădăcină a lui f. Atunci α este o rădăcină de ordin $e \geqslant 2$ a lui f dacă și numai dacă este o rădăcină de ordin $e - 1$ a polinomului Df.**

Demonstrație. Dacă α este rădăcină de multiplicitate e a lui f, atunci

$$f = (X - \alpha)^e g, \ g \in K[X], \ g(\alpha) \neq 0.$$

Luînd derivata formală, avem:

$$Df = D(X - \alpha)^e \cdot g + (X - \alpha)^e Dg = e(X - \alpha)^{e-1} g + (X - \alpha)^e Dg =$$
$$= (X - \alpha)^{e-1}(eg + (X - \alpha) Dg) = (X - \alpha)^{e-1} h,$$

unde $h = eg + (X - \alpha) Dg$. Cum $h(\alpha) = eg(\alpha) + (\alpha - \alpha) Dg(\alpha) = eg(\alpha) \neq 0$ rezultă că α este rădăcină de ordin $e - 1$ al lui Df.

Reciproc, presupunem că α este rădăcină de multiplicitate $e - 1$ a lui Df și fie e' ordinul de multiplicitate al rădăcinii α a lui f. Conform primei părți a demonstrației α este rădăcină de ordin $e' - 1$ al lui Df. Deci $e - 1 = e' - 1$, de unde $e' = e$.

8.5. *Consecință.* **Fie $f \in K[X]$ și $\alpha \in K$. Următoarele afirmații sînt echivalente:**

1) α este rădăcină multiplă de ordin e a lui f.

2) $f(\alpha) = Df(\alpha) = \ldots = D^{e-1}f(\alpha) = 0$ și $D^e f(\alpha) \neq 0$.

Exemple.

1. Fie $f = X^4 - 3X^3 + X^2 + 4 \in \mathbb{Q}[X]$. Să cercetăm dacă polinomul f admite rădăcini multiple. Conform Consecinței 8.3. rădăcinile multiple ale lui f se găsesc printre rădăcinile polinomului Df. Cum $Df = 4X^3 - 9X^2 + 2X = X(4X^2 - 9X + 2)$, rădăcinile polinomului Df sînt 0,2 și 1/4. Cum $f(0) \neq 0$, $f(2) = 0$ și $f(1/4) \neq 0$, singura rădăcină multiplă a polinomului f este $\alpha = 2$. Cum $D^2f = 12X^2 - 18X + 2$ și $D^2f(2) = 14 \neq 0$, rezultă că $\alpha = 2$ este rădăcină dublă a lui f.

2. Fie $f = aX^4 + bX^3 + 1 \in \mathbb{Q}[X]$. Să determinăm a, $b \in \mathbb{Q}$ astfel încît $(X-1)^2 \mid f$. Dacă $(X-1)^2 \mid f$ rezultă că $\alpha = 1$ este rădăcină a lui f de ordin $e \geqslant 2$. Conform Teoremei 8.4 trebuie ca $f(1) = 0$ și $Df(1) = 0$. Cum $Df = 4aX^3 + 3bX^2$, /avem $a + b + 1 = 0$, și $4a + 3b = 0$, de unde $a = 3$ și $b = -4$.

3. Fie $f = aX^2 + bX + c \in \mathbb{C}[X]$. Să vedem ce condiție trebuie să satisfacă coeficienții a, b, c astfel încît f să admită o rădăcină dublă. Avem $Df = 2aX + b$. Polinomul Df are rădăcina $\alpha = -b/2a$. Punînd condiția ca $f(\alpha) = 0$ se găsește $b^2 - 4ac = 0$, ceea ce s-a stabilit cu alte mijloace în clasele anterioare.

§ 9. RELAȚII ÎNTRE RĂDĂCINI ȘI COEFICIENȚI

Fie f un polinom de grad m cu coeficienți numerici

$$f = a_m X^m + a_{m-1}X^{m-1} + \ldots + a_1 X + a_0, \quad a_m \neq 0.$$

Putem presupune că $f \in \mathbb{C}[X]$. Conform Consecinței 3.3 numărul rădăcinilor distincte din $\mathbb{C}$ ale polinomului f este $\leqslant m$. Din Consecința 7.2 rezultă că există $z_1, z_2, \ldots z_m \in \mathbb{C}$ unic determinați astfel încît

$$f = a_m(X - z_1)(X - z_2) \ldots (X - z_m). \qquad (*)$$

Să observăm că

$$f(z_i) = a_m(z_i - z_1)(z_i - z_2) \ldots (z_i - z_i) \ldots (z_i - z_m) = 0, \quad 1 \leqslant i \leqslant m$$

deci $z_1, z_2, \ldots, z_m$ sînt rădăcini din $\mathbb{C}$ ale lui f. Reciproc, dacă $z \in \mathbb{C}$ este rădăcină a lui f, atunci

$$0 = f(z) = a_m(z - z_1)(z - z_2) \ldots (z - z_m),$$

deci există i, $1 \leqslant i \leqslant m$, astfel încît $z - z_i = 0$, de unde $z = z_i$. Așadar, $z_1, z_2, \ldots, z_m$ sînt rădăcinile din $\mathbb{C}$ (nu neapărat distincte) ale polinomului f.

Dacă ordinul de multiplicitate al rădăcinii z_1 este e_1, atunci $f = (X - z_1)^{e_1}g$, $g \in \mathbb{C}[X]$, $g(z_1) \neq 0$. Dacă factorul $X - z_1$ din descompunerea (*) se repetă de e_1' ori, atunci (*) se mai scrie $f = (X - z_1)^{e_1'}h$, $h(z_1) \neq 0$. Avem $e_1 = e_1'$. În adevăr, dacă $e_1 > e_1'$, atunci din $(X - z_1)^{e_1}g = (X - z_1)^{e_1'}h$ rezultă $(X - z_1)^{e_1 - e_1'}g = h$,
de unde

$$0 \neq h(z_1) = (z_1 - z_1)^{e_1 - e_1'}g(z_1) = 0.$$

Contradicție. La fel se exclude inegalitatea $e_1 < e_1'$, de unde $e_1 = e_1'$. Același raționament se face pentru fiecare z_i. Am demonstrat:

9.1. *Teoremă.* **Dacă $f = a_m X^m + \ldots + a X + a_0$ este un polinom de grad m cu coeficienți numerici, atunci f se scrie în mod unic sub forma:**

$$f = a_m(X - z_1)(X - z_2) \ldots (X - z_m)$$

unde $z_1, z_2, \ldots, z_m$ sînt rădăcinile (nu neapărat distincte) din $\mathbb{C}$ ale lui f. Fiecare factor $X - z_i$ apare în această descompunere de e_i ori, unde e_i este ordinul de multiplicitate al rădăcinii z_i.

Numerele complexe $z_1, z_2, \ldots, z_m$ din relația (*), cu repetițiile date de multiplicitatea lor, sînt numite *rădăcinile polinomului f.*

Între coeficienții unui polinom și rădăcinile sale există o legătură intimă ce se descrie prin relații cunoscute sub numele de *formulele lui Viète.*

Înainte de a formula rezultatul general, să considerăm cazurile $m = 2$ și $m = 3$.

Din egalitatea $a_2X^2 + a_1X + a_0 = a_2(X - z_1)(X - z_2)$, $a_2 \neq 0$, deducem

$$a_2X^2 + a_1X + a_0 = a_2X^2 - a_2(z_1 + z_2)X + a_2z_1z_2$$

și prin identificarea coeficienților, obținem:

$$z_1 + z_2 = -\frac{a_1}{a_2},$$

$$z_1z_2 = \frac{a_0}{a_2}.$$

Din egalitatea $a_3X^3 + a_2X^2 + a_1X + a_0 = a_3(X - z_1)(X - z_2)(X - z_3)$, $a_3 \neq 0$, deducem
$a_3X^3 + a_2X^2 + a_1X + a_0 = a_3X^3 - a_3(z_1 + z_2 + z_3)X^2 + a_3(z_1z_2 + z_1z_3 + z_2z_3)X - a_3z_1z_2z_3$ și prin identificarea coeficienților, obținem:

$$z_1 + z_2 + z_3 = -\frac{a_2}{a_3},$$

$$z_1z_2 + z_1z_3 + z_2z_3 = \frac{a_1}{a_3},$$

$$z_1z_2z_3 = -\frac{a_0}{a_3}.$$

În general:

10.7. *Teoremă* **(formulele lui Viète). Numerele complexe** $z_1, z_2, \ldots, z_m$ **sînt rădăcinile polinomului cu coeficienți numerici** $f = a_m X^m + a_{m-1}X^{m-1} + \ldots + a_1 X + a_0$, $a_m \neq 0$, **dacă și numai dacă:**

$$(1) \qquad z_1 + z_2 \ldots + z_m = -\frac{a_{m-1}}{a_m},$$

$$(2) \qquad z_1z_2 + z_1z_3 + \ldots + z_{m-1}z_m = \frac{a_{m-2}}{a_m},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$(i) \qquad z_1z_2 \ldots z_i + \ldots + z_{m-i+1} \ldots z_m = (-1)^i \frac{a_{m-i}}{a_m},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$(m) \qquad z_1z_2 \ldots z_m = (-1)^m \frac{a_0}{a_m}.$$

Demonstrație. În relația (*) se dezvoltă produsul $a_m \prod_{i=1}^{m} (X - z_i)$ și apoi se identifică coeficienți. Să observăm că pentru a constitui membrul stîng al relației (i), $1 \leqslant i \leqslant m$, se fac toate combinările de $z_1, z_2, \ldots, z_m$ luate cîte i, în total relația i avînd C_m^i termeni ce sînt produse de i factori.

Reciproc, presupunem că numerele complexe $z_1, z_2, \ldots, z_m$ satisfac relațiile (1) — (m) și fie

$$g = a_m(X - z_1)(X - z_2) \ldots (X - z_m).$$

Desfăcînd parantezele și ținînd cont de relațiile (1) — (m) avem:

$$g = a_mX^m - (z_1 + z_2 + \ldots + z_m)X^{m-1} + \ldots + (-1)^m z_1z_2 \ldots z_m =$$

$$= a_mX^m + a_m \frac{a_{m-1}}{a_m} X^{m-1} + \ldots + (-1)^m a_m(-1)^m \frac{a_0}{a_m} =$$

$$= a_mX^m + a_{m-1}X^{m-1} + \ldots + a_0 = f.$$

Cum $f(z_i) = g(z_i) = 0$, $1 \leqslant i \leqslant m$,
rezultă că $z_1, z_2, \ldots, z_m$ sînt rădăcini ale polinomului f.

Formulele lui Viète pot folosi la aflarea rădăcinilor unui polinom atunci cînd se dă o informație suplimentară despre acestea.

Exemple.

1. Să aflăm rădăcinile polinomului $f = 2X^3 - X^2 - 7X - 3$, știind că $z_1 + z_2 = 1$.

Formulele lui Viète pentru polinomul f sînt

$$z_1 + z_2 + z_3 = 1/2,$$
$$z_1z_2 + z_1z_3 + z_2z_3 = -7/2,$$
$$z_1z_2z_3 = 3/2.$$

Cum $z_1 + z_2 = 1$, din prima relație deducem că $z_3 = -1/2$. Din ultima relație scoatem $z_1z_2 = -3$ și cum $z_1 + z_1 = 1$, obținem $z_1 = (1 + \sqrt{3})/2$, $z_2 = (1 - \sqrt{3})/2$.

2. Să se determine parametrul λ și rădăcinile polinomului $f = X^4 - 2X^3 - 6X^2 + \lambda X - 3$ știind că $z_1z_2 = 3$. Formulele lui Viète pentru polinomul f sînt:

$$z_1 + z_2 + z_3 + z_4 = 2,$$
$$z_1z_2 + (z_1 + z_2)(z_3 + z_4) + z_3z_4 = -6,$$
$$z_1z_2(z_3 + z_4) + (z_1 + z_2)z_3z_4 = -\lambda,$$
$$z_1z_2z_3z_4 = -3,$$

unde s-au făcut în relațiile a 2-a și a 3-a grupări de factori ce sînt adesea utile. Din ultima relație, după ce punem $z_1z_2 = -3$, se scoate $z_3z_4 = -1$. Acum primele două relații mai pot fi scrise

$$(z_1 + z_2) + (z_3 + z_4) = 2,$$
$$(z_1 + z_2)(z_3 + z_4) = -8,$$

de unde $z_1 + z_2 = 4$, $z_3 + z_4 = -2$. Din a 3-a relație se scoate acum $\lambda = 10$. Cum $z_1 + z_2 = 4$ și $z_1z_2 = 3$, avem $z_1 = 3$, $z_2 = 1$. De asemenea, din $z_3 + z_4 = -2$ și $z_3z_4 = -1$, deducem $z_3 = -1 + \sqrt{2}$ și $z_4 = -1 - \sqrt{2}$.

§ 10. RĂDĂCINI ALE POLINOAMELOR CU COEFICIENȚI RAȚIONALI

1. Rădăcini conjugate ale polinoamelor cu coeficienți raționali. Fie d un întreg liber de pătrate și $\mathbf{Q}(\sqrt{d})$ corpul numerelor pătratice de forma $a + b\sqrt{d}$, cu $a, b \in \mathbf{Q}$ (v. Cap. IV, § 4). Dacă $z \in \mathbf{Q}(\sqrt{d})$, $z = a + b\sqrt{d}$, atunci numărul $z^* = a - b\sqrt{d}$ s-a numit *conjugatul* numărului pătratic z. Avem:

$$(z_1 + z_2)^* = z_1^* + z_2^*, \qquad (z_1 \cdot z_2)^* = z_1^* \, z_2^*$$

oricare ar fi $z_1, z_2 \in \mathbf{Q}(\sqrt{d})$ (v. § 5, Cap. I) și evident

$$z^* = z \Leftrightarrow z \in \mathbf{Q}.$$

10.1. *Teoremă.* **Fie** f **un polinom cu coeficienți raționali,** $f = a_mX^m + a_{m-1}X^{m-1} + \ldots + a_1X + a_0$, $a_m \neq 0$.

Dacă f **admite ca rădăcină numărul pătratic** $z = a + b\sqrt{d}$, **atunci conjugatul lui** z, $z^* = a - b\sqrt{d}$, **este, de asemenea, rădăcină a lui** f. **Dacă** $b \neq 0$, **atunci** f **se divide prin polinomul**

$$X^2 - 2aX + a^2 - db^2 \in \mathbf{Q}[X].$$

Demonstrație. Conform ipotezei avem $f(z) = 0$, deci

$$a_m z^m + a_{m-1}z^{m-1} + \ldots + a_1 z + a_0 = 0,$$

de unde

$$0 = 0^* = (a_m z^m + a_{m-1}z^{m-1} + \ldots + a_1 z + a_0)^* =$$
$$= (a_m z^m)^* + (a_{m-1}z^{m-1})^* + \ldots + (a_1 z)^* + a_0^* =$$
$$= a_m (z^*)^m + a_{m-1}(z^*)^{m-1} + \ldots + a_1 z^* + a_0.$$

Rezultă că $f(z^*) = 0$, deci

$$f(a + b\sqrt{d}) = 0 \Rightarrow f(a - b\sqrt{d}) = 0.$$

Dacă $b \neq 0$, atunci $z \neq z^*$, deci f se divide prin polinomul $(X - z)(X - z^*) = X^2 - 2aX + a^2 - db^2$ (v. Ex. R—2, § 3).

Exemple

1. Să aflăm rădăcinile polinomului $f = X^3 - aX^2 + 6X + 70$ știind că admite rădăcina $z_1 = 2 + 3\sqrt{2}$. Conform Teoremei 10.1, f admite și rădăcina $z_2 = 2 - 3\sqrt{2}$ și se divide prin polinomul $X^2 - (z_1 + z_2)X + z_1 z_2 = X^2 - 4X - 14$. Aplicînd algoritmul împărțirii, găsim $f = (X^2 - 4X - 14)(X - 5)$, deci $z_3 = 5$.
2. Să găsim rădăcinile polinomului $f = X^4 - 8X^3 + 32X^2 - 92X + 91$, știind că admite rădăcina $z_1 = 1 + 2\sqrt{-3}$. Conform Teoremei 10.1 (sau Teoremei 6.6) f admite și rădăcina $z_2 = 1 - 2\sqrt{-3}$. De asemenea, f se divide prin $X^2 - (z_1 + z_2)X + z_1 z_2 = X^2 - 2X + 13$. Efectuînd împărțirea, găsim $f = (X^2 - 2X + 13)(X^2 - 6X + 7)$, deci f admite și rădăcinile $z_3 = 3 + \sqrt{2}$ și $z_4 = 3 - \sqrt{2}$.

2. **Rădăcini raționale ale polinoamelor cu coeficienți întregi.** Prezentăm în continuare condiții necesare pentru ca un număr rațional (resp. întreg) să fie rădăcină a unui polinom cu coeficienți întregi.

10.2. *Teoremă.* **Fie $f \in \mathbb{Z}[X]$, $f = a_m X^m + a_{m-1}X^{m-1} + \ldots + a_1 X + a_0$, $a_m \neq 0$. Dacă $\alpha = p/q$ este o rădăcină rațională a lui f, unde p și q sînt relativ prime, atunci $p \mid a_0$ și $q \mid a_m$.**

Demonstrație. Cum $f(\alpha) = 0$, avem:

$$a_m \frac{p^m}{q^m} + a_{m-1}\frac{p^{m-1}}{q^{m-1}} + \ldots + a_1 \frac{p}{q} + a_0 = 0.$$

După înmulțirea cu q^m, din egalitatea precedentă deducem că

$$a_0 q^m = -p(a_m p^{m-1} + \ldots + a_1 q^{m-1})$$

și

$$a_m p^m = -q(a_{m-1}p^{m-1} + \ldots + a_0 q^{m-1}),$$

de unde rezultă că $p \mid a_0 q^m$ și $q \mid a_m p^m$.

Cum $(p, q) = 1$, rezultă că $(p, b^m) = 1$ și $(p^m, q) = 1$ (v. § 4, Cap. I). Acum din $p \mid a_0 q^m$ și $(p, q^m) = 1$, rezultă că $p \mid a_0$. Analog se arată că $q \mid a_m$.

10.3. *Consecință.* **Fie $f \in \mathbb{Z}[X]$, $f = a_m X^m + \ldots + a_1 X + a_0$, $a_m \neq 0$. Dacă a este o rădăcină întreagă a polinomului f, atunci $a \mid a_0$.** Altfel spus, **rădăcinile întregi ale unui polinom cu coeficienți întregi se găsesc printre divizorii termenului liber al lui f.**

Demonstrație. Avem $a = a/1$ și se aplică teorema precedentă.

Exemple.

1. Să aflăm rădăcinile raționale ale polinomului $f = 2X^3 + 3X^2 + 6X - 4$. Avem $m = 3$, $a_m = 2$ și $a_0 = -4$. Divizorii lui a_0 sînt ± 1, ± 2, ± 4 iar ai lui a_3 sînt ± 1, ± 2. Deci pentru rădăcinile raționale ale lui f avem următorii candidați:

$$1,\ -1,\ 2,\ -2,\ 4,\ -4,\ \frac{1}{2},\ -\frac{1}{2}.$$

Din tabelul

x	-4	-2	-1	$-1/2$	$1/2$	1	2	4
$f(x)$	-108	-26	-9	$-35/4$	0	7	36	324

deducem că $\alpha = 1/2$ este singura rădăcină rațională a lui f.

2. Să aflăm rădăcinile raționale ale polinomului $f = X^5 - 2X^4 - 4X^3 + 4X^2 - 5X + 6$. Avem $m = 5$, $a_m = 1$ și $a_0 = 6$.
Cum f este unitar ($a_5 = 1$) și o rădăcină rațională a/b satisface $b \mid a_5$, rezultă că orice rădăcină rațională a lui f este întreagă și se găsește printre divizorii lui $a_0 = 6$. Aceștia sînt ± 1, ± 2, ± 3, ± 6. Se constată că $f(1) = 0$, $f(-1) \neq 0$, $f(2) \neq 0$, $f(-2) = 0$, $f(3) = 0$, $f(-3) \neq 0$, $f(6) \neq 0$ și $f(-6) \neq 0$. Așadar, rădăcinile raționale ale lui f sînt 1, -2 și 3.

3. **Ecuații algebrice.** Fie $f \in \mathbb{C}[X]$, $f = a_m X^m + a_{m-1}X^{m-1} + \ldots + a_1 X + a_0$, $a_m \neq 0$. Egalitatea:

$$a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0 = 0 \qquad (*)$$

se numește *ecuație algebrică* (cu coeficienți numerici) în necunoscuta x, asociată polinomului f. *Gradul* ecuației algebrice (*) este prin definiție gradul polinomului f, *rădăcinile (soluțiile)* ecuației (*) sînt prin definiție rădăcinile polinomului f. O rădăcină $\alpha \in C$ a ecuației (*) se numește *simplă* (*dublă*, *triplă*, ...) dacă este rădăcină simplă (resp. dublă, triplă, ...) a polinomului f. Conform teoremei fundamentale a algebrei orice ecuație algebrică cu coeficienți complecși admite cel puțin o rădăcină complexă. Conform Teoremei 9.1 orice ecuație algebrică de grad m admite m rădăcini complexe (egale sau distincte). Rezolvarea (determinarea rădăcinilor) ecuațiilor de grad 1 și 2 este o problemă relativ simplă și se cunoaște din clasele anterioare. Pentru unele ecuații de grad superior, de tipuri particulare, se cunosc metode speciale de rezolvare. De asemenea, toate metodele de determinare a rădăcinilor polinoamelor sînt aplicabile la ecuații algebrice.

Exerciţii

1. Fie $f, g \in \mathbf{Z}_5[X]$, $f = \hat{2}X^3 + \hat{4}X^2 + \hat{3}X + \hat{1}$ şi $g = \hat{3}X^3 + \hat{2}X^2 + X + \hat{3}$. Calculaţi $f + g$ şi fg.

2. Fie $f, g \in \mathbf{Z}_6[X]$, $f = \hat{3}X^2 + \hat{3}X + \hat{3}$, $g = \hat{2}X^3 + \hat{4}X + \hat{2}$. Calculaţi fg.

3. Fie $f \in \mathbf{Z}_3[X]$, $f = X^3 + \hat{2}X^2 + X + \hat{1}$. Determinaţi toate polinoamele $g = aX^3 + bX^2 + cX + d \in \mathbf{Z}_3[X]$ cu proprietatea: $\bar{g} = \bar{f}$.

4. Enumeraţi rădăcinile din $\mathbf{Z}_6$ ale polinomului $f = \hat{3}X^2 + \hat{3}X \in \mathbf{Z}_6[X]$.

5. Să se determine două polinoame f şi g de grad 1, $f, g \in \mathbf{Q}[X]$, astfel încît

$$f^2 + g^2 = X^2 + 1, \qquad f(2)g(2) = 2.$$

6. Determinaţi gradul polinomului $f \in \mathbf{R}[X]$,

$$f = (\lambda^2 - 3\lambda + 2)X^3 + (\lambda^2 - 4\lambda + 3)X^2 + (\lambda^2 - 1)X + 1, \text{ unde}$$

λ este un parametru real.

7. Să se determine două polinoame f şi g de grad 1, $f, g \in \mathbf{Z}[X]$, astfel încît

$$(X^2 + 2X + 2)f + (X^2 + 3X + 3)g = 1.$$

8. Fie K un corp comutativ şi $f_1, f_2, f_3 \in K[X]$, grad $f_i = i$, $1 \leqslant i \leqslant 3$. Arătaţi că egalitatea

$$\alpha_1 f_1 + \alpha_2 f_2 + \alpha_3 f_3 = 0 \qquad (\alpha_i \in K)$$

este posibilă numai în cazul $\alpha_1 = \alpha_2 = \alpha_3 = 0$. Generalizare.

9. Fie $f \in \mathbf{R}[X]$, grad $f \leqslant 2$. Dacă există trei numere reale diferite α_1, α_2, α_3 astfel încît

$$f(\alpha_i) = 0, \qquad i = 1, 2, 3,$$

atunci f este egal cu polinomul zero. Generalizare.

10. Fie $f, g \in \mathbf{C}[X]$, $f = 2X^4 + (1 - 2i)X^3 + (4 - 2i)X^2 + (1 + i)X - 2i$, $g = X^2 - iX + 2$.
Aflaţi cîtul şi restul împărţirii lui f prin g.

11. Fie $f, g \in \mathbf{Z}_5[X]$, $f = \hat{3}X^5 + X^3 + \hat{2}X + \hat{4}$, $g = \hat{2}X^3 + \hat{3}X^2 + \hat{1}$. Aflaţi cîtul şi restul împărţirii lui f prin g.

12. Fie $f, g \in \mathbf{Q}[X]$, $f = 2X^4 - 3X^2 + aX + b$, $g = X^2 - 2X + 3$. Să se determine a şi b astfel încît $g \mid f$.

13. Fie $f \in \mathbf{Z}[X]$, $f = a_0 + a_1X + a_2X^2 + a_3X^3$. Determinaţi coeficienţii polinomului f dacă

$$f(1) + f(2) + \ldots + f(n) = n^4, \qquad \forall n > 0.$$

14. Fie $f \in \mathbf{C}[X]$, $f = a + bX + X^2$. Determinaţi a şi b astfel încît f să dividă polinomul $X^4 + 1$.

15. Să se efectueze împărţirile cu rest în inelul $\mathbf{Q}[X]$:

1) $2X^4 - 3X^3 + 4X^2 - 5X + 6$ la $X^2 - 3X + 1$;
2) $X^3 - 3X^2 - X - 1$ la $3X^2 - 2X + 1$.

16. Să se afle $f \in \mathbf{R}[X]$, grad $f = 3$, dacă împărţit la $X^2 - 3X$ dă restul $6X - 15$ şi împărţit la $X^2 - 5X + 8$ dă restul $2X - 7$.

17. Fie $f \in \mathbf{Q}[X]$, $f = X^5 - 5X^4 + 18X^3 - 15X^2 + X + 4$. Folosind schema lui Horner, calculaţi $f(3)$.

18. Calculaţi cu schema lui Horner cîtul şi restul împărţirii polinomului

$$f \in \mathbf{Z}_7[X], f = \hat{5}X^4 + \hat{3}X^2 + X + \hat{2}, \text{ prin } X + \hat{5}.$$

19. Folosind schema lui Horner să se afle $f(a)$, unde

$$f \in \mathbf{C}[X], \ f = X^5 + (1 + 2i)X^4 - (1 + 3i)X^2 + 7 \quad \text{şi} \quad a = -2 - i.$$

20. Folosind schema lui Horner să se dezvolte polinomul f după puterile lui $X + a$, unde:

1) $f = X^4 + 2X^3 - 3X^2 - 4X + 1 \in \mathbf{R}[X]$, $a = -1$,
2) $f = X^4 + 2iX^3 - (1 + i)X^2 - 3X + 7 + i \in \mathbf{C}[X]$, $a = -i$.

21. Să se determine $a, b, c, d \in \mathbf{R}$ astfel încît polinomul $f = X^4 - X^3 + aX^2 + bX + c$ împărţit prin $X^2 + d$ să dea restul X iar împărţit prin $X^2 - d$ să dea restul $-X$.

22. Să se determine un polinom $f \in \mathbf{R}[X]$ de grad 5 ştiind că $f + 8$ este divizibil prin $(X + 1)^3$ iar $f - 8$ este divizibil prin $(X - 1)^3$.

23. Fie $f \in \mathbf{R}[X]$, $f = X^{2n} - 12X^n + 32$. Să se determine n astfel încît f să se dividă prin $X - 2$.

24. Folosind schema lui Horner să se descompună în fracţii simple funcţiile raţionale:

1) $F(x) = \dfrac{x^3 - x + 1}{(x - 2)^5}$, $\qquad x \in \mathbf{R} \setminus \{2\}$,

2) $G(x) = \dfrac{x^4 - 2x^2 + 3}{(x + 1)^3}$, $\qquad x \in \mathbf{R} \setminus \{-1\}$.

25. Folosind de două ori schema lui Horner, să se arate că polinomul $f = X^{n+1} - (n + 1)X + n$, $n \geqslant 1$, se divide prin $(X - 1)^2$. Să se afle cîtul.

26. Dacă polinomul $f \in \mathbf{Z}[X]$ admite două rădăcini întregi de parităţi diferite, atunci $f(k)$ este par, $k \in \mathbf{Z}$.

27. Folosind algoritmul lui Euclid, să se găsească c.m.m.d.c. al polinoamelor

a) $f = X^4 + 3X^3 + X^2 - 2$ şi $g = X^3 + 2X^2 + 2X + 1$ din $\mathbf{Q}[X]$;
b) $f = X^5 + X^2 - X + 1$ şi $g = 3X^4 - 5X^3 + 8X + 1$ din $\mathbf{Q}[X]$;
c) $f = nX^{n+1} - (n + 1)X^n + 1$ şi $g = X^n - nX + n - 1$ din $\mathbf{Q}[X]$;
d) $f = X^4 + X^2 + \hat{2}X + \hat{2}$ şi $g = X^2 + \hat{3}X + \hat{6}$ din $\mathbf{Z}_7[X]$;
e) $f = X^4 + \hat{2}X^3 + X + \hat{2}$ şi $g = X^4 + X^3 + \hat{2}X + \hat{2}$ din $\mathbf{Z}_3[X]$.

28. Fie $f, g \in \mathbf{Q}[X]$, $f = X^3 + aX^2 + 11X + 6$ şi $g = X^3 + bX^2 + 14X + 8$. Să se determine a şi b astfel încît f şi g să aibă un divizor comun de grad 2.

29. Să se determine $\lambda, \mu \in \mathbf{Q}$ astfel încît (f, g) să fie un polinom de grad 2, unde

$$f = 2X^3 - 7X^2 + \lambda X + 3, \quad g = X^3 - 3X^2 + \mu X + 3.$$

30. Să se descompună în factori ireductibili peste $\mathbf{R}$ şi peste $\mathbf{C}$ polinoamele $X^4 + 4$, $X^6 + 27$.

31. Să se descompună în factori ireductibili peste $\mathbf{Z}_5$ polinomul

$$f = X^4 + X^3 + \hat{2}X^2 + X + \hat{1}.$$

32. Fie $f \in \mathbf{Q}[X]$, $f = X^3 - 2$.
1) Arătaţi că f este ireductibil peste $\mathbf{Q}$.
2) Descompuneţi în factori ireductibili polinomul f peste $\mathbf{R}$ şi peste $\mathbf{C}$.

33. Să se determine ordinul de multiplicitate al rădăcinii:
a) $\alpha = 2$ pentru $f = X^5 - 5X^4 + 7X^3 - 2X^2 + 4X - 8 \in \mathbf{Q}[X]$;
b) $\alpha = -2$ pentru $f = X^5 + 7X^4 + 16X^3 + 8X^2 - 16X - 16 \in \mathbf{Q}[X]$.

34. Să se determine λ astfel ca polinomul $f = X^5 + \lambda X^2 + \lambda Y + 1 \in \mathbf{Q}[X]$ să admită ca rădăcină dublă pe $\alpha = -1$.

35. Să se determine a și b astfel încît polinomul $aX^4 + bX^3 + 1 \in \mathbf{Q}[X]$ să fie divizibil prin $(X - 1)^2$.

36. Arătați că polinomul $f = X^{2n} - nX^{n+1} + nX^{n-1} - 1$ și $g = X^{2n+1} - (2n + 1)X^{n+1} + (2n + 1)X^n - 1 \in \mathbf{Q}[X]$ admit pe $\alpha = 1$ ca rădăcină triplă.

37. Să se arate că pentru orice n polinomul $f \in \mathbf{C}[X]$,

$$f = \frac{1}{n!}X^n + \frac{1}{(n-1)!}X^{n-1} + \ldots + \frac{1}{2!}X^2 + X + 1$$

are numai rădăcini simple.

38. Fie $f \in \mathbf{R}[X]$, $f = (a + 2)X^3 - (a^2 + 2a + 1)X + a^2 + a - 1$, $a \neq -2$.
1) Să se afle rădăcinile polinomului f știind că una dintre ele nu depinde de a.
2) Pentru ce valoare a lui a polinomul f admite o rădăcină dublă?

39. Arătați că oricare ar fi m, $n \geqslant 1$, polinomul $f = mX(1 - X^n) - nX(1 - X^m) \in \mathbf{Z}[X]$ admite pe 1 ca rădăcină dublă.

40. Să se determine ordinul de multiplicitate al rădăcinii -1 a polinomului $f = X^5 + 6X^4 + 14X^3 + 16X^2 + 9X + 2$. Aflați apoi toate rădăcinile lui f.

41. Aflați rădăcinile polinomului $f \in \mathbf{R}[X]$,
$f = X^4 - 4X^2 + 4aX - 1$ știind că admite o rădăcină dublă.

42. Să se afle rădăcinile polinomului f știind că acestea satisfac relația indicată:
a) $f = 3X^3 + 7X^2 - 18X + 8$, $z_1 + z_2 = -3$;
b) $f = X^3 - 13X + 12a^3$, $z_1 - z_2 = 2a$;
c) $f = X^4 - (4 + 5i)X^3 - 4(3 - 5i)X^2 + 6(4 + 5i)X + 36$, $z_1 \cdot z_2 = z_3 \cdot z_4$;
d) $f = X^3 - 12X^2 + aX + 60$, $z_1^2 = z_2^2 + z_3^2$.

43. Fie $f \in \mathbf{Q}[X]$, $f = X^5 - 5X^4 - 5X^3 + 25X^2 + 4X - 20$. Aflați rădăcinile lui f știind că $z_1 + z_2 = z_3 + z_4 = 0$.

44. Fie x_1, x_2, x_3 rădăcinile polinomului $f \in \mathbf{R}[X]$, $f = 2X^3 + 2X^2 - 3X - 1$. Construiți polinomul g ale cărui rădăcini sînt: $y_1 = (x_2 + x_3)/x_1$, $y_2 = (x_1 + x_3)/x_2$, $y_3 = (x_1 + x_2)/x_3$.

45. Fie x_1, x_2, x_3 rădăcinile polinomului $f \in \mathbf{R}[X]$, $f = X^3 - 5X + 2$. Calculați $x_1^5 + x_2^5 + x_3^5$.

46. Fie x_1, x_2, x_3 rădăcinile polinomului $f \in \mathbf{R}[X]$, $f = X^3 + aX + b$.
Construiți polinomul g ale cărui rădăcini sînt x_1^2, x_2^2, x_3^2.

47. Să se afle rădăcinile polinomului $f \in \mathbf{R}[X]$, $f = 2X^3 - 12X^2 + 6X + a$ știind că acestea formează o progresie aritmetică.

48. Să se determine rădăcinile polinomului $f \in \mathbf{R}[X]$, $f = 2X^3 - 7X^2 + 7X + a$, știind că acestea formează o progresie geometrică.

49. Fie $f \in \mathbf{C}[X]$, $f = X^4 + 6X^3 + 8X^2 + aX + b$.
Să se determine a și b știind că trei dintre rădăcinile lui f sînt în progresie aritmetică și a patra este egală cu suma celorlalte.

50. Să se afle rădăcinile polinomului $f \in \mathbf{R}[X]$, $f = X^3 - 3X + 2$ știind că $z_1 - z_2 = 0$.

51. Să se afle rădăcinile polinomului $f \in \mathbf{Q}[X]$ știind că admite rădăcina indicată:
a) $f = X^4 + aX^3 - X^2 - 2X + b$, $z_1 = 2 + \sqrt{2}$;
b) $f = X^4 - 2X^3 + aX^2 + bX + 1$, $z_1 = (3 - \sqrt{5})/2$.

52. Fie $f \in \mathbf{C}[X]$, $f = X^3 - 6X - 6$. Să se arate că $\alpha = \sqrt[3]{2} + \sqrt[3]{4}$ este rădăcină a lui f. Aflați toate rădăcinile lui f.

53. Fie $f \in \mathbf{R}[X]$, $f = X^4 + aX^3 + 3X^2 + 2X + b$. Să se afle a și b știind că f admite rădăcina $z = 1 + i$.

54. Fie $f \in \mathbf{R}[X]$, $f = 2X^3 - aX^2 + 2aX - a + 2$. Să se afle a știind că f admite rădăcina $z = 2 + \sqrt{3}\,i$.

55. Să se arate că polinomul $f = X^{3n} + X^{3m+1} + X^{3p+2}$ se divide prin polinomul $g = X^2 + X + 1$.

56. Fie $f \in \mathbf{R}[X]$, $f = X^4 + 2X^3 + 3X^2 + aX + b$. Să se determine rădăcinile lui f știind că una dintre ele este $z = 1 + i$.

57. Fie $f \in \mathbf{Z}[X]$, $f = a_mX^m + \ldots + a_1X + a_0$ și $\alpha = a/b$ o rădăcină rațională ireductibilă a lui f. Arătați că pentru orice $k \in \mathbf{Z}$, $a - kb$ divide $f(k)$. În particular $a - b$ divide pe $f(1)$ și $a + b$ divide pe $f(-1)$.

58. Să se afle rădăcinile raționale ale polinoamelor $4X^4 - 7X^2 - 5X - 1$,
$X^4 + 4X^3 - 2X^2 - 12X + 9$, $6X^4 + 19X^3 - 7X^2 - 26X + 12$.

59. Să se găsească rădăcinile raționale ale polinomului $f = 12X^3 - 8X^2 + 13X - 2 \in \mathbf{Z}[X]$.

60. Să se demonstreze că un polinom $f \in \mathbf{Z}[X]$ nu are rădăcini întregi dacă $f(0)$ și $f(1)$ sînt numere impare.

* * *

61.* Fie K mulțimea tuturor polinoamelor $f \in \mathbf{R}[X]$ de forma $a + bX$, $a, b \in \mathbf{R}$. Dacă $f, g \in K$, definim $f * g = r$, unde r este restul împărțirii prin $X^2 + 1$ al polinomului fg. Arătați că adunarea uzuală a polinoamelor, împreună cu înmulțirea $K \times K \to K$, $(f, g) \to f * g$, conferă mulțimii K o structură de corp izomorf cu $\mathbf{C}$.

62.* Repetînd construcția de la Ex. 61* luînd $\mathbf{Z}_3[X]$ în loc de $\mathbf{R}[X]$ și $X^2 + \hat{1} \in \mathbf{Z}_3[X]$ în loc de $X^2 + 1$, să se arate că se obține un corp K cu 9 elemente. Alcătuiți tabla adunării și tabla înmulțirii acestui corp.

63.* Fie $f \in \mathbf{R}[X]$, $f = a_mX^m + \ldots + a_1X + a_0$, $a_m \neq 0$, și $z = u + iv \in \mathbf{C}$ o rădăcină a lui f de multiplicitate e. Atunci $z = u - iv$ este rădăcină a lui f de multiplicitate e.

64.* Fie $f \in \mathbf{Q}[X]$, $f = a_mX^m + \ldots + a_1X + a_0$, $a_m \neq 0$, și $z = a + b\sqrt{d}$ un număr pătratic care este rădăcină a lui f. Arătați că $a - b\sqrt{d}$ este rădăcină a lui f de aceeași multiplicitate ca și z.

65.* Fie $z \in \mathbf{C}$ o rădăcină a unui polinom $f \in \mathbf{Q}[X]$, grad $f > 0$. Dacă $g \in \mathbf{Q}[X]$ este un polinom diferit de 0 de grad minim printre polinoamele diferite de 0 din $\mathbf{Q}[X]$ care admit pe z ca rădăcină, atunci g este ireductibil peste $\mathbf{Q}$.

66.* Fie $f \in \mathbf{Z}[X]$, $f \neq 0$. Să se arate că nu există trei întregi diferiți a, b, c astfel încît $f(a) = b$, $f(b) = c$, $f(c) = a$.

67.* Fie $f \in \mathbf{R}[X]$, grad $f > 3$ și $g = f(X) - f(2a - X)$. Dacă $D^1f(a) = 0$, atunci g este divizibil prin $(X - a)^3$.

68.* Determinați polinoamele $f \in \mathbf{R}[X]$ cu proprietatea:

$$xf(x) = (x - 3)\,f(x + 1), \qquad \forall x \in \mathbf{R}$$

69.* Să se determine $n \in \mathbf{N}$ și $f \in R[X]$, grad $f = n$, astfel încît

$$f = \mathrm{D}^1 f \cdot \mathrm{D}^2 f \cdot \ldots \mathrm{D}^n f.$$

70.* Fie $f \in \mathbf{R}[X]$, grad $f = n$. Dacă $\mathrm{D}f$ divide pe f, atunci $f = \frac{a}{n!}(X - c)^n$.

71.* Fie $f \in \mathbf{R}[X]$, $f = X^4 - 4X^3 + 6X^2 + aX + b$. Dacă rădăcinile x_1, x_2, x_3, x_4 ale lui f sînt reale, atunci $x_1 = x_2 = x_3 = x_4$.

72.* Fie $f \in \mathbf{Q}[X]$ astfel încît $\sqrt[3]{2}$ este rădăcină a lui f. Arătați că f se divide cu polinomul $X^3 - 2$.

73.* Determinați rădăcinile polinomului $f \in \mathbf{Q}[X]$,

$$f = 1 + X + \frac{1}{2!}X(X+1) + \ldots + \frac{1}{n!}X(X+1)\ldots(X+n-1).$$

74.* Fie $f \in \mathbf{Q}[X]$, $f = X^n + X^{n-1} + \ldots + X + 1$.
Dacă x_1, x_2, ..., x_n sînt rădăcinile (din $\mathbf{C}$) ale lui f, calculați

$$S_n = \sum_{k=1}^{n} \frac{1}{x_k - 2}.$$

75.* Fie $f \in \mathbf{Z}[X]$. Dacă gradul lui f este par iar coeficienții săi sînt impari, atunci f nu admite rădăcini raționale.

76.* Fie $f = \sum_{i=0}^{n} a_i(X - b_i)^n$, unde a_i, $b_i \in \mathbf{R}$ și $b_i \neq b_j$ pentru $i \neq j$. Dacă $f(x) = a$, $\forall x \in \mathbf{R}$, atunci $a = 0$.

77.* Fie f, g, $h \in K[X]$. Arătați:

1) Dacă $(f, g) = 1$ și $(f, h) = 1$, atunci $(f, gh) = 1$.
2) Dacă $f \mid h$, $g \mid h$ și $(f, g) = 1$, atunci $fg \mid h$.
3) Dacă $f \mid gh$ și $(f, g) = 1$, atunci $f \mid h$.

78.* Fie π_1, ..., π_n, π_1', ..., $\pi_{n'}'$, polinoame ireductibile unitare din $K[X]$ astfel încît $\pi_1 \pi_2 \ldots \pi_n = \pi_1' \pi_2' \ldots \pi_{n'}'$. Arătați că $n = n'$ și că există $\sigma \in \mathfrak{S}_n$ astfel încît $\pi_i = \pi_{\sigma(i)}'$, $1 \leqslant i \leqslant n$.

79.* Fie f, $g \in \mathbf{Z}[X]$, $h = fg$ și $p > 0$ un număr prim. Dacă toți coeficienții lui h se divid prin p atunci cel puțin unul din polinoamele f, g are toți coeficienții divizibili prin p.

80.* (criteriul lui Eisenstein). Fie $f \in \mathbf{Z}[X]$, $f = a_n X^n + \ldots + a_1 X + a_0$, $a_n \neq 0$, $n > 0$. Dacă există un număr prim p astfel încît $p \mid a_i$, $0 \leqslant i < n$, p nu divide a_n și p^2 nu divide a_0, atunci f este ireductibil peste $\mathbf{Q}$.

§ 1. LEGI DE COMPOZIȚIE EXTERNE

Legile de compoziție studiate în capitolele anterioare sînt aplicații de tipul

$$\varphi : M \times M \to M, \qquad (x, y) \to \varphi(x, y) \in M,$$

unde M este o mulțime nevidă. Ele se numesc încă *legi de compoziție interne*.

Noțiunea de lege de compoziție internă este un caz particular al unui concept mai general:

1.1. *Definiție.* **Fie Ω și M două mulțimi nevide. O aplicație**

$$\psi : \Omega \times M \to M, \qquad (\omega, x) \to \psi(\omega, x) \in M$$

se numește *lege de compoziție externă* **pe M cu** *operatori* **în Ω.**

Pentru *compusul* $\psi(\omega, x)$ al elementului $x \in M$ cu *operatorul* $\omega \in \Omega$ se folosește de regulă notația multiplicativă, $\psi(\omega, x) = \omega x$. Mulțimea Ω poartă numele de *domeniul operatorilor* legii de compoziție externe ψ. O lege de compoziție internă pe M poate fi privită ca o lege de compoziție externă cu domeniul operatorilor $\Omega = M$.

Exemple

1. *Înmulțirea matricelor cu scalari.* Fie $\Omega = \mathbf{R}$ și $M = M_2(\mathbf{R})$. Pentru orice $\alpha \in \mathbf{R}$ și $A \in M_2(\mathbf{R})$, $A = (a_{ij})$ definim matricea $\alpha A \in M_2(\mathbf{R})$,

$$\alpha A \overset{\text{def}}{=} \begin{pmatrix} \alpha a_{11} & \alpha a_{12} \\ \alpha a_{21} & \alpha a_{22} \end{pmatrix}.$$

Se obține astfel o lege de compoziție externă pe $M_2(\mathbf{R})$ cu operatori în $\mathbf{R}$,

$$\mathbf{R} \times M_2(\mathbf{R}) \to M_2(\mathbf{R}), \qquad (\alpha, A) \to \alpha A,$$

numită *înmulțirea matricelor cu scalari.*
Operațiile de adunare și înmulțire ale corpului $\mathbf{R}$, adunarea matricelor din $M_2(\mathbf{R})$ și înmulțirea matricelor cu scalari sînt legate prin:

$$\mathrm{S}_1) \quad (\alpha + \beta)A = \alpha A + \beta A,$$
$$\mathrm{S}_2) \quad \alpha(A + B) = \alpha A + \alpha B,$$
$$\mathrm{S}_3) \quad \alpha(\beta A) = (\alpha\beta)A,$$
$$\mathrm{S}_4) \quad 1 \cdot A = A$$

oricare ar fi α, $\beta \in \mathbf{R}$ și A, $B \in M_2(\mathbf{R})$.

Pentru exemplificare, să demonstrăm S_3). Avem:

$$\alpha(\beta A) = \alpha \begin{pmatrix} \beta a_{11} & \beta a_{12} \\ \beta a_{21} & \beta a_{22} \end{pmatrix} = \begin{pmatrix} \alpha(\beta a_{12}) & \alpha(\beta a_{11}) \\ \alpha(\beta a_{21}) & \alpha(\beta a_{22}) \end{pmatrix} = \begin{pmatrix} (\alpha\beta)a_{11} & (\alpha\beta)a_{12} \\ (\alpha\beta)a_{21} & (\alpha\beta)a_{22} \end{pmatrix} = (\alpha\beta)A.$$

2. *Înmulțirea polinoamelor cu scalari.* Fie $\Omega = \mathbf{R}$ și $M = \mathbf{R}[X]$. Pentru orice $\alpha \in \mathbf{R}$ și $f \in \mathbf{R}[X]$, $f = a_0 + a_1X + \ldots + a_mX^m$, definim polinomul $\alpha f \in \mathbf{R}[X]$,

$$\alpha f \overset{\text{def}}{=} \alpha a_0 + \alpha a_1 X + \ldots + \alpha a_m X^m.$$

Se obține astfel o lege de compoziție externă pe $\mathbf{R}[X]$ cu operatori în $\mathbf{R}$,

$$\mathbf{R} \times \mathbf{R}[X] \to \mathbf{R}[X], \ (\alpha, f) \to \alpha f,$$

numită *înmulțirea polinoamelor cu scalari.*

Înmulțirea polinoamelor cu scalari are proprietățile:

$S_1)$ $(\alpha + \beta)f = \alpha f + \beta f$,
$S_2)$ $\alpha(f + g) = \alpha f + \alpha g$,
$S_3)$ $\alpha(\beta f) = (\alpha\beta)f$,
$S_4)$ $1 \cdot f = f$,

oricare ar fi $\alpha, \beta \in \mathbf{R}$ și $f, g \in \mathbf{R}[X]$. Astfel:

$$(\alpha + \beta)f = (\alpha + \beta)a_0 + (\alpha + \beta)a_1X + \ldots + (\alpha + \beta)a_mX^m =$$
$$= \alpha a_0 + \beta a_0 + \alpha a_1 X + \beta a_1 X + \ldots + \alpha a_m X^m + \beta a_m X^m =$$
$$= \alpha a_0 + \alpha a_1 X + \ldots + \alpha a_m X^m + \beta a_0 + \beta a_1 X + \ldots + \alpha a_m X^m = \alpha f + \beta f.$$

3. *Înmulțirea vectorilor de poziție cu scalari.* Fie Π un plan euclidian în care fixăm un punct O ce va fi numit *origine*. La fiecare punct P al planului Π se asociază segmentul orientat x cu originea în O și extremitatea în P, numit *vectorul de poziție* al punctului P (relativ la originea O).

Să notăm cu V mulțimea tuturor vectorilor de poziție astfel obținuți. Dacă $x, y \in V$, se notează cu $x + y$ vectorul de poziție al celui de-al patrulea vîrf al paralelogramului determinat de x și y (v. Fig. VI.1).
Se obține astfel o lege de compoziție internă pe V,

$$V \times V \to V, \quad (x, y) \to x + y,$$

numită *adunarea geometrică* a vectorilor de poziție. Procedeul descris mai sus de aflare a sumei geometrice a doi vectori de poziție este cunoscut sub numele de „*regula paralelogramului*". Considerații geometrice simple arată că $(V, +)$ este grup abelian; elementul neutru al acestui grup este vectorul de poziție al originii O iar opusul lui x este vectorul de poziție al simetricului lui P în raport cu O (v. Fig. VI.1).

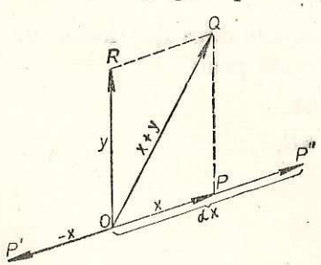


Fig. VI.1

Dacă α este un număr real, iar x este vectorul de poziție al punctului P, atunci *produsul* lui α cu x, notat cu αx, este prin definiție vectorul de poziție al punctului P'' determinat prin condițiile:

1) lungimea lui OP'' este egală cu produsul dintre $|\alpha|$ și lungimea lui OP;

2) P'' se găsește pe dreapta determinată de O și P de aceeași parte cu P față de O dacă $\alpha > 0$, în partea opusă cînd $\alpha < 0$.

Se obține astfel o lege de compoziție externă pe V cu operatori în $\mathbf{R}$,

$$\mathbf{R} \times V \to V, \quad (\alpha, x) \to \alpha x,$$

numită *înmulțirea vectorilor de poziție cu scalari.*

Această lege de compoziție are proprietățile:

$S_1)$ $(\alpha + \beta)x = \alpha x + \beta x$,
$S_2)$ $\alpha(x + y) = \alpha x + \alpha y$,
$S_3)$ $\alpha(\beta x) = (\alpha\beta)x$,
$S_1)$ $1 \cdot x = x$

oricare ar fi $\alpha, \beta \in \mathbf{R}$ și $x, y \in V$.

§ 2. DEFINIȚIA SPAȚIULUI VECTORIAL

2.1. *Definiție.* **Fie K un corp. Se numește *spațiu vectorial* (peste corpul K) un grup abelian $(V, +)$ pe care este dată o lege de compoziție externă cu operatori în K,**

$$K \times V \to V, \quad (\alpha, u) \to \alpha u,$$

ce satisface axiomele:

$S_1)$ $(\alpha + \beta)u = \alpha u + \beta u$,
$S_2)$ $\alpha(u + v) = \alpha u + \alpha v$,
$S_3)$ $\alpha(\beta u) = (\alpha\beta)u$,
$S_4)$ $1 \cdot u = u$

oricare ar fi $\alpha, \beta \in K$, $u, v \in V$.

Se folosește următoarea terminologie:
— elementele lui V se numesc *vectori* iar operația grupului $(V, +)$ se numește *adunarea vectorilor*;
— elementele lui K se numesc *scalari* iar legea de compoziție externă $K \times V \to V$ se numește *înmulțirea vectorilor cu scalari*;
— elementul neutru al grupului $(V, +)$ se numește *vectorul zero*, notat cu 0, ca și scalarul zero;
— cînd $K = \mathbf{R}$ sau $K = \mathbf{C}$ se spune că V este *spațiu vectorial real*, respectiv *complex*;
— spațiile vectoriale se numesc încă *spații liniare.*

Să observăm că S_1) și S_2) consemnează faptul că înmulțirea vectorilor cu scalari este distributivă față de adunarea scalarilor, respectiv adunarea vectorilor iar S_3) descrie o lege de asociativitate care angajează atît înmulțirea vectorilor cu scalari cît și înmulțirea scalarilor.

Notă. Inițial noțiunea de vector a apărut în Mecanică și Fizică, avînd ca model geometric segmentul orientat și fiind folosit pentru a descrie fenomene caracterizate prin amplitudine, direcție și sens. Ulterior, aria de aplicabilitate a noțiunii de vector s-a lărgit considerabil. Definiția dată mai sus spațiului vectorial dă posibilitatea de a pune în „postura" de vector obiecte de natură variată. De exemplu: matrice, funcții și polinoame în matematică, secvențe finite de 0 și 1 în teoria codurilor, sisteme ordonate $(x_1, x_2, ..., x_n)$ de numere reale în economie.

Exemple

1. *Spațiul vectorial* $\mathbf{R}^n$. Fie $n > 1$ un număr natural. Se notează cu $\mathbf{R}^n$ mulțimea tuturor sistemelor ordonate de n numere reale,

$$x = (a_1, a_2, ..., a_n), \qquad (a_i \in \mathbf{R}).$$

Dacă $\alpha \in \mathbf{R}$ și $x, y \in \mathbf{R}^n$, $x = (a_1, a_2, ..., a_n)$, $y = (b_1, b_2, ..., b_n)$ atunci:

$$x = y \overset{\text{def}}{\Leftrightarrow} a_i = b_i, \qquad 1 \leqslant i \leqslant n,$$

$$x + y \overset{\text{def}}{=} (a_1 + b_1, a_2 + b_2, ..., a_n + b_n),$$

$$\alpha x = \overset{\text{def}}{=} (\alpha a_1, \alpha a_2, ..., \alpha a_n).$$

O verificare directă arată că legea de compoziție internă

$$\mathbf{R}^n \times \mathbf{R}^n \to \mathbf{R}^n, \qquad (x, y) \to x + y$$

este asociativă și comutativă. Dacă $0 = (0, 0, ..., 0)$, atunci oricare ar fi $x \in \mathbf{R}^n$, $x = (a_1, a_2, ..., a_n)$ avem

$$0 + x = (0 + a_1, 0 + a_2, ..., 0 + a_n) = (a_1, a_2, ..., a_n) = x = x + 0,$$

iar dacă punem

$$-x \overset{\text{def}}{=} (-a_1, -a_2, ..., -a_n)$$

avem și

$$x + (-x) = (a_1 + (-a_1), a_2 + (-a_2), ..., a_n + (-a_n)) = 0 = (-x) + x.$$

Rezultă că $(\mathbf{R}^n, +)$ este grup abelian.

De asemenea, se verifică că legea de compoziție externă

$$\mathbf{R} \times \mathbf{R}^n \to \mathbf{R}^n, \qquad (\alpha, x) \to \alpha x$$

satisface axiomele S_1) —S_4) din definiția spațiului vectorial. Astfel,

$$\forall \alpha \in \mathbf{R} \text{ și } x, y \in \mathbf{R}^n, \; x = (a_1, a_2, ..., a_n),$$
$$y = (b_1, b_2, ..., b_n)$$

avem:

$$\alpha(x + y) = \alpha(a_1 + b_1, a_2 + b_2, ..., a_n + b_n) = (\alpha(a_1 + b_1), \alpha(a_2 + b_2), ...,$$
$$..., \alpha(a_n + b_n) = (\alpha a_1 + \alpha b_1, \alpha a_2 + \alpha b_2, ..., \alpha a_n + \alpha b_n) = (\alpha a_1, \alpha a_2, ...,$$
$$..., \alpha a_n) + (\alpha b_1, \alpha b_2, ..., \alpha b_n) = \alpha x + \alpha y,$$

deci axioma S_2) este verificată.

Elementele lui $\mathbf{R}^n$ se numesc *vectori* (linie) *n-dimensionali* iar $\mathbf{R}^n$ se numește *spațiul aritmetic real* de dimensiune n, sau *spațiul vectorilor linie n-dimensionali*. Dacă $x \in \mathbf{R}^n$, $x = (a_1, a_2, ..., a_n)$, atunci a_i se numește *componenta* de rang i a lui x, $1 \leqslant i \leqslant n$.

În unele aplicații este avantajos să dăm vectorii lui $\mathbf{R}^n$ sub formă de coloane,

$$x = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \qquad (a_i \in \mathbf{R}).$$

În acest caz $\mathbf{R}^n$ va fi numit *spațiul vectorilor coloană n-dimensionali*. Analog, se introduce spațiul aritmetic $\mathbf{C}^n$ și de asemenea spațiul vectorial K^n, K corp oarecare.

2. Mulțimea $M_2(\mathbf{R})$ a matricelor pătratice de ordin 2 cu coeficienți reali formează spațiu vectorial peste corpul $\mathbf{R}$ în raport cu adunarea și înmulțirea matricelor cu scalari. În adevăr, $(M_2(\mathbf{R}), +)$ este grup abelian iar înmulțirea matricelor cu scalari satisface axiomele S_1)—S_4) (v. § 1).

3. Mulțimea $\mathbf{R}[X]$ a polinoamelor în nedeterminata X cu coeficienți reali formează spațiu vectorial peste corpul $\mathbf{R}$ în raport cu adunarea și înmulțirea polinoamelor cu scalari (v. § 1).

4. Mulțimea V a vectorilor de poziție ai punctelor dintr-un plan cu originea într-un punct O a planului formează spațiu vectorial peste corpul $\mathbf{R}$ în raport cu adunarea și înmulțirea cu scalari (v. § 1).

5. *Spațiul vectorial* 0. Fie K un corp. Pe grupul abelian zero, $0 = \{0\}$, introducem legea de compoziție externă

$$K \times 0 \to 0, \qquad (\alpha, 0) \to \alpha \cdot 0 = 0.$$

Se conferă astfel grupului abelian 0 o structură de spațiu vectorial peste K, numit spațiul vectorial *zero*.

Fie V un spațiu vectorial peste corpul K. Cum $(V, +)$ este grup abelian, pentru adunarea vectorilor sînt valabile regulile de calcul dintr-un grup abelian. Să adăugăm la acestea următoarele proprietăți specifice ale operațiilor cu vectori:

a) Fie $\alpha \in K$ și $x \in V$. Atunci:

$$\boxed{\alpha x = 0 \Leftrightarrow \alpha = 0 \text{ sau } x = 0}.$$

În adevăr, fie $\alpha = 0$ și $y = 0 \cdot x$. Atunci

$$y = 0x = (0 + 0)x = 0x + 0x = y + y,$$

de unde

$$y = y + 0 = y + (y + (-y)) = (y + y) + (-y) = y + (-y) = 0,$$

deci $0x = 0$ și analog se arată că $\alpha 0 = 0$.

Reciproc, presupunem că $\alpha x = 0$. Dacă $\alpha \neq 0$, atunci

$$x = 1 \cdot x = (\alpha^{-1}\alpha)x = \alpha^{-1}(\alpha x) = \alpha^{-1} 0 = 0.$$

b) Oricare ar fi $\alpha \in K$ și $x \in V$, avem:

$$\boxed{(-\alpha)x = \alpha(-x) = -\alpha x,\ (-\alpha)(-x) = \alpha x}$$

În adevăr,

$$0 = \alpha 0 = \alpha(x + (-x)) = \alpha x + \alpha(-x),$$

de unde rezultă că $\alpha(-x)$ este opusul vectorului x deci $\alpha(-x) = -\alpha x$. Analog se arată că $(-\alpha)x = -\alpha x$ și atunci

$$(-\alpha)(-x) = -(\alpha(-x)) = -(-\alpha x) = \alpha x.$$

c) Oricare ar fi $\alpha, \beta \in K$ și $x, y \in V$ avem:

$$\boxed{(\alpha - \beta)x = \alpha x - \beta x,\ \alpha(x - y) = \alpha x - \alpha y}$$

În adevăr,

$$(\alpha - \beta)x = (\alpha + (-\beta))x = \alpha x + (-\beta)x = \alpha x - \beta x$$

și la fel se demonstrează a doua regulă de distributivitate.

§ 3. DEPENDENȚĂ ȘI INDEPENDENȚĂ LINIARĂ. BAZĂ

1. Bază. a) Fie V spațiul vectorilor de poziție dintr-un plan euclidian. Fie v_1 și v_2 doi vectori de poziție diferiți de zero și necoliniari (v. fig. VI.2).

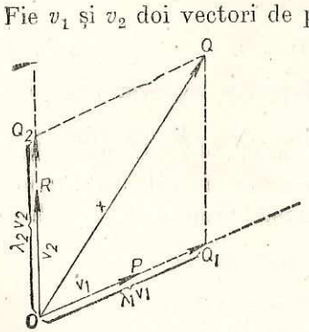


Fig. VI.2

Sistemul de vectori $\mathbf{B}$ format cu v_1 și v_2, $\mathbf{B} = (v_1, v_2)$ are proprietățile:

1) $\forall x \in V$, $\exists \lambda_1, \lambda_2 \in \mathbf{R}$ astfel încît $x = \lambda_1 v_1 + \lambda_2 v_2$,

2) Dacă $\alpha_1 v_1 + \alpha_2 v_2 = 0$, cu $\alpha_1, \alpha_2 \in \mathbf{R}$, atunci $\alpha_1 = \alpha_2 = 0$.

În adevăr, paralelele duse prin extremitatea Q a vectorului x la dreptele definite de v_1 și v_2 determină pe acestea punctele Q_1 și Q_2 respectiv. Există $\lambda_1, \lambda_2 \in \mathbf{R}$ astfel încît $OQ_1 = \lambda_1 v_1$ și $OQ_2 = \lambda_2 v_2$. Din construcție rezultă că suma geometrică a vectorilor de poziție $\lambda_1 v_1$ și $\lambda_2 v_2$ este egală cu x, deci

$$x = \lambda_1 v_1 + \lambda_2 v_2$$

și 1) este astfel verificat. Dacă 2) nu este adevărat, există $\alpha_1, \alpha_2 \in \mathbf{R}$, $\alpha_1 \neq 0$ sau $\alpha_2 \neq 0$, astfel încît

$$\alpha_1 v_1 + \alpha_2 v_2 = 0.$$

Presupunem că $\alpha_1 \neq 0$. Atunci deducem că $v_1 = -\alpha_1^{-1}\alpha_2 v_2$, deci v_1 și v_2 sînt coliniari, contrar ipotezei.

b) În spațiul vectorial $\mathbf{R}^3$ să considerăm vectorii v_1, v_2, v_3, unde $v_1 = (1, 1, 1)$, $v_2 = (0, 1, 1)$ și $v_3 = (0, 0, 1)$. Fie $\mathbf{B}$ sistemul format cu v_1, v_2, v_3, $\mathbf{B} = (v_1, v_2, v_3)$. Vectorul zero al spațiului $\mathbf{R}^3$ este $(0, 0, 0)$ și va fi notat cu 0 ca și scalarul zero.

Sistemul de vectori $\mathbf{B}$ are proprietățile:

1) $\forall x \in \mathbf{R}^3$, $\exists \lambda_1, \lambda_2, \lambda_3 \in \mathbf{R}$ astfel încît

$$x = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3.$$

2) Dacă $\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 = 0$, cu $\alpha_1, \alpha_2, \alpha_3 \in \mathbf{R}$, atunci $\alpha_1 = \alpha_2 = \alpha_3 = 0$.

În adevăr, fie $x \in \mathbf{R}^3$, $x = (a_1, a_2, a_3)$. Pentru a arăta că 1) este adevărat trebuie să determinăm $\lambda_1, \lambda_2, \lambda_3 \in \mathbf{R}$ astfel încît

$$x = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3.$$

Avem:

$$\begin{aligned}(a_1, a_2, a_3) = x = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 = \lambda_1(1, 1, 1) + \lambda_2(0, 1, 1) + \\ + \lambda_3(0, 0, 1) = (\lambda_1, \lambda_1, \lambda_1) + (0, \lambda_2, \lambda_2) + \\ + (0, 0, \lambda_3) = (\lambda_1, \lambda_1 + \lambda_2, \lambda_1 + \lambda_2 + \lambda_3)\end{aligned}$$

de unde

$$\begin{cases} \lambda_1 = a_1, \\ \lambda_1 + \lambda_2 = a_2, \\ \lambda_1 + \lambda_2 + \lambda_3 = a_3. \end{cases}$$

Rezultă că $\lambda_1 = a_1$, $\lambda_2 = a_2 - a_1$, $\lambda_3 = a_3 - a_2$ și 1) este verificat.

Fie acum $\alpha_1, \alpha_2, \alpha_3 \in \mathbf{R}$ astfel încît

$$\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 = 0.$$

Deducem că

$$(\alpha_1, \alpha_1 + \alpha_2, \alpha_1 + \alpha_2 + \alpha_3) = (0, 0, 0),$$

deci

$$\begin{cases} \alpha_1 = 0, \\ \alpha_1 + \alpha_2 = 0, \\ \alpha_1 + \alpha_2 + \alpha_3 = 0, \end{cases}$$

de unde $\alpha_1 = \alpha_2 = \alpha_3 = 0$.

Exemple ca cele de mai sus justifică introducerea următorului concept:

3.1. *Definiție.* **Fie V un spațiu vectorial peste corpul K. Un sistem $\mathbf{B} = (e_1, e_2, ..., e_n)$ de vectori $e_i \in V$, $1 \leqslant i \leqslant n$, se numește** *bază* a lui V dacă:

1) $\forall x \in V$, $\exists \lambda_1, \lambda_2, ..., \lambda_n \in K$ **astfel încît**

$$x = \lambda_1 e_1 + \lambda_2 e_2 + ... \lambda_n e_n;$$

2) **Dacă** $\alpha_1 e_1 + \alpha_2 e_2 + ... + \alpha_n e_n = 0$, cu $\alpha_1, \alpha_2, ..., \alpha_n \in K$, **atunci** $\alpha_1 = \alpha_2 = ... = \alpha_n = 0$.

Din cele de mai sus rezultă că orice sistem $\mathbf{B} = (v_1, v_2)$ format cu doi vectori diferiți de zero necoliniari formează o bază a spațiului V al vectorilor de poziție dintr-un plan euclidian.

Sistemul $\mathbf{B} = (v_1, v_2, v_3)$, unde $v_1 = (1, 1, 1)$, $v_2 = (0, 1, 1)$, $v_3 = (0, 0, 1)$ formează o bază a spațiului vectorial $\mathbf{R}^3$.

2. Dependență și independență liniară. Strîns legate de noțiunea de bază a unui spațiu vectorial V peste un corp K sînt conceptele următoare:

i) Dacă $v_1, v_2, ..., v_m \in V$, atunci un vector de forma

$$\lambda_1 v_1 + \lambda_2 v_2 + ... + \lambda_m v_m \qquad (\lambda_i \in K)$$

se numește *combinație liniară* (cu coeficienți în K) de vectorii $v_1, v_2, ..., v_m$; scalarii $\lambda_1, \lambda_2, ..., \lambda_m$ se numesc *coeficienții* combinației liniare.

ii) Spunem că un vector $x \in V$ este *combinație liniară* (cu coeficienți în K) de vectorii $v_1, v_2, ..., v_m$ dacă există $\lambda_1, \lambda_2, ..., \lambda_m \in K$ astfel încît

$$x = \lambda_1 v_1 + \lambda_2 v_2 + ... + \lambda_m v_m = \sum_{i=1}^{m} \lambda_i v_i.$$

Spunem că vectorii $v_1, v_2, ..., v_m$ formează un *sistem de generatori* pentru spațiul vectorial V dacă orice vector $x \in V$ se poate reprezenta ca o combinație liniară de $v_1, v_2, ..., v_m$:

$$\forall x \in V, \exists \lambda_1, \lambda_2, ..., \lambda_m \in K \text{ astfel încît } x = \sum_{i=1}^{m} \lambda_i v_i.$$

iii) Spunem că sistemul de vectori $v_1, v_2, ..., v_m$ este *liniar independent* (peste K) dacă

$$\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_m v_m = 0 \Rightarrow \alpha_1 = \alpha_2 = ... = \alpha_m = 0.$$

În caz contrar spunem că vectorii $v_1, v_2, ..., v_m$ sînt *liniar dependenți* (peste K). Așadar, vectorii $v_1, v_2, ..., v_m$ sînt liniar dependenți (peste K) dacă există $\alpha_1, \alpha_2, ..., \alpha_m \in K$, *nu toți nuli*, astfel încît

$$\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_m v_m = 0.$$

O egalitate de forma:

$$\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_m v_m = 0, \qquad (\alpha_i \in K)$$

se numește *relație de dependență liniară* a vectorilor $v_1, v_2, ..., v_m$; dacă cel puțin unul dintre scalarii $\alpha_1, \alpha_2, ..., \alpha_m$ este diferit de zero spunem că avem o relație de dependență liniară *nebanală*.

Așadar, vectorii $v_1, v_2, ..., v_n$ sînt liniar independenți dacă și numai dacă singura relație de dependență liniară a lor este cea banală. De asemenea, un sistem de vectori $\mathbf{B}$ este bază a lui V dacă și numai dacă $\mathbf{B}$ este sistem de generatori liniar independent.

Exerciții rezolvate

R—1 În spațiul vectorial $\mathbf{R}^3$ considerăm vectorii $v_1 = (a, 1, 1)$, $v_2 = (1, a, 1)$, $v_3 = (1, 1, a)$, unde a este parametru real.

1) Arătați că sistemul de vectori v_1, v_2, v_3 este liniar dependent dacă și numai dacă $a = 1$ sau $a = -2$.

2) Dacă $a \neq 1$ și $a \neq -2$, atunci $\mathbf{B} = (v_1, v_2, v_3)$ este bază a lui V. Cînd $a = -1$, reprezentați vectorul $v = (3, 2, 5)$ ca o combinație liniară de v_1, v_2, v_3.

Soluție. 1) Fie $\alpha_1, \alpha_2, \alpha_3 \in \mathbf{R}$ astfel încît

$$\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 = 0.$$

Atunci.

$$(a\alpha_1 + \alpha_2 + \alpha_3, \quad \alpha_1 + a\alpha_2 + \alpha_3, \quad \alpha_1 + \alpha_2 + a\alpha_3) = (0, 0, 0),$$

ceea ce este echivalent cu:

$$(S_0) \begin{cases} a\alpha_1 + \alpha_2 + \alpha_3 = 0, \\ \alpha_1 + a\alpha_2 + \alpha_3 = 0, \\ \alpha_1 + \alpha_2 + a\alpha_3 = 0. \end{cases}$$

Sistemul omogen (S_0) în necunoscutele $\alpha_1, \alpha_2, \alpha_3$ admite soluții nebanale dacă și numai dacă

$$\Delta = \begin{vmatrix} a & 1 & 1 \\ 1 & a & 1 \\ 1 & 1 & a \end{vmatrix} = 0$$

deci dacă și numai dacă $(a + 2)(a - 1)^2 = 0$. Rezultă că vectorii v_1, v_2, v_3 sînt liniar dependenți dacă și numai dacă $a = -2$ sau $a = 1$.

2) Fie $x \in \mathbf{R}^3$, $x = (a_1, a_2, a_3)$. Să arătăm că se pot determina scalarii $\lambda_1, \lambda_2, \lambda_3 \in \mathbf{R}$ astfel încît

$$x = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3.$$

Trebuie să avem

$$(a\lambda_1 + \lambda_2 + \lambda_3, \quad \lambda_1 + a\lambda_2 + \lambda_3, \quad \lambda_1 + \lambda_2 + a\lambda_3) = (a_1, a_2, a_3)$$

ceea ce este echivalent cu:

$$(S) \begin{cases} a\lambda_1 + \lambda_2 + \lambda_3 = a_1, \\ \lambda_1 + a\lambda_2 + \lambda_3 = a_2, \\ \lambda_1 + \lambda_2 + a\lambda_3 = a_3. \end{cases}$$

Cum $a \neq 1$ și $a \neq -2$ determinantul Δ al sistemului (S) este diferit de zero,

$$\Delta = (a+2)(a-1)^2 \neq 0.$$

În acest caz sistemul (S) admite soluție (chiar unică!). Conform regulii lui Cramer acesta este:

$$\lambda_1 = \frac{a^2-1}{\Delta} a_1 + \frac{1-a}{\Delta} a_2 + \frac{1-a}{\Delta} a_3,$$

$$\lambda_2 = \frac{1-a}{\Delta} a_1 + \frac{a^2-1}{\Delta} a_1 + \frac{1-a}{\Delta} a_3,$$

$$\lambda_3 = \frac{1-a}{\Delta} a_1 + \frac{1-a}{\Delta} a_2 + \frac{a^2-1}{\Delta} a_3.$$

Cînd $a = -1$ și $a_1 = 3$, $a_2 = -2$, $a_3 = 5$ avem $\Delta = 4$ și aplicînd formulele de mai sus găsim $\lambda_1 = 3/2$, $\lambda_2 = 4$, $\lambda_3 = 1/2$, deci

$$v = (3, -2, 5) = \frac{3}{2} v_1 + 4v_2 + \frac{1}{2} v_3.$$

R—2 Fie K un corp, Γ un inel și $f : K \to \Gamma$ un morfism de inele.

Pe grupul abelian $(\Gamma, +)$ al inelului Γ definim legea de compoziție externă

$$(*) \qquad K \times \Gamma \to \Gamma, \ (\alpha, x) \to \alpha x \overset{\text{def}}{=} f(\alpha)x.$$

1) Arătați că Γ este spațiu vectorial peste corpul K în raport cu adunarea inelului Γ și legea de compoziție externă (*).

2) Cînd $K = \mathbf{R}$, $\Gamma = M_2(\mathbf{R})$ și f este morfismul

$$f : \mathbf{R} \to M_2(\mathbf{R}), \qquad f(\alpha) = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}, \qquad \forall \alpha \in \mathbf{R},$$

arătați că spațiul vectorial obținut coincide cu cel de la Exp. 2 § 2.

3) Arătați că matricele $E_{ij} \in M_2(\mathbf{R})$,

$$E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \ E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \ E_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \ E_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

formează o bază a spațiului vectorial de la pct. 2).

4) Luînd $K = \mathbf{R}$, $\Gamma = \mathbf{C}$ și $f : \mathbf{R} \to \mathbf{C}$, $f(\alpha) = \alpha$, $\forall \alpha \in \mathbf{R}$, deduceți că $\mathbf{C}$ este spațiu vectorial peste $\mathbf{R}$ și indicați o bază a acestuia.

5) Luînd $K = \mathbf{Q}$, $\Gamma = \mathbf{Q}(\sqrt{d})$, d liber de pătrate și $f : \mathbf{Q} \to \mathbf{Q}(\sqrt{d})$, $f(\alpha) = \alpha$, $\forall \alpha \in \mathbf{Q}$, deduceți că $\mathbf{Q}(\sqrt{d})$ este spațiu vectorial peste $\mathbf{Q}$ și indicați o bază a acestuia.

Soluție. 1) Cum f este morfism de inele, avem:

$f(\alpha + \beta) = f(\alpha) + f(\beta)$, $\forall \alpha, \beta \in K$,

$f(\alpha\beta) = f(\alpha)f(\beta)$, $\forall \alpha, \beta \in K$,

$f(1) = e$.

Folosind proprietățile înmulțirii unui inel și definiția legii de compoziție externe (*) pentru orice $\alpha, \beta \in K$ și $x, y \in \Gamma$ avem:

$(\alpha + \beta)x = f(\alpha + \beta)x = (f(\alpha) + f(\beta))x = f(\alpha)x + f(\beta)x = \alpha x + \beta x$,

$\alpha(x + y) = f(\alpha)(x + y) = f(\alpha)x + f(\alpha)y = \alpha x + \alpha y$,

$\alpha(\beta x) = \alpha(f(\beta)x) = f(\alpha)(f(\beta)x) = (f(\alpha)f(\beta))x = f(\alpha\beta)x = (\alpha\beta)x$,

$1 \cdot x = f(1)x = ex = x$,

unde 1 este elementul unitate al corpului K și e este elementul unitate al inelului Γ. Rezultă că Γ este spațiu vectorial peste K.

2) Pentru orice $\alpha, \beta \in \mathbf{R}$ avem:

$$f(\alpha + \beta) = \begin{pmatrix} \alpha+\beta & 0 \\ 0 & \alpha+\beta \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} + \begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix} = f(\alpha) + f(\beta),$$

$$f(\alpha\beta) = \begin{pmatrix} \alpha\beta & 0 \\ 0 & \alpha\beta \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}\begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix} = f(\alpha)f(\beta),$$

$$f(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

deci f este morfism de inele. Conform definiției legii de compoziție (*), pentru orice $\alpha \in \mathbf{R}$ și $A \in M_2(\mathbf{R})$, $A = (a_{ij})$ avem:

$$\alpha A = f(\alpha)A = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} \alpha a_{11} & \alpha a_{12} \\ \alpha a_{21} & \alpha a_{22} \end{pmatrix},$$

deci legea de compoziție (*) coincide cu înmulțirea matricelor cu scalari. Așadar, spațiul vectorial obținut coincide cu cel de la Exp. 2, § 2.

3) Dacă $A \in M_2(\mathbf{R})$, $A = (a_{ij})$, atunci

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & a_{12} \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ a_{21} & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & a_{22} \end{pmatrix} =$$

$$= a_{11}E_{11} + a_{12}E_{12} + a_{21}E_{21} + a_{22}E_{22},$$

deci $E_{11}, E_{12}, E_{21}, E_{22}$ formează un sistem de generatori ai lui $M_2(\mathbf{R})$ ca spațiu vectorial peste $\mathbf{R}$.

Fie $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in \mathbf{R}$ astfel încît

$$\alpha_{11}E_{11} + \alpha_{12}E_{12} + \alpha_{21}E_{21} + \alpha_{22}E_{22} = 0.$$

Rezultă că

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

deci $\alpha_{11} = \alpha_{12} = \alpha_{21} = \alpha_{22} = 0$. Rezultă că $E_{11}, E_{12}, E_{21}, E_{22}$ formează un sistem de vectori liniari independenți peste $\mathbf{R}$.

4) Cum orice număr complex z se scrie sub forma

$$z = a + bi = a \cdot 1 + b\mathrm{i}, \qquad a, b \in \mathbf{R}$$

rezultă că 1, i formează un sistem de generatori al lui $\mathbf{C}$ ca spațiu vectorial peste $\mathbf{R}$. Dacă

$$a \cdot 1 + b \cdot \mathrm{i} = 0 = 0 \cdot 1 + 0 \cdot \mathrm{i}, \qquad a, b \in \mathbf{R}$$

din definiția egalității numerelor complexe rezultă că $a = b = 0$. Așadar 1 și i formează o bază a lui $\mathbf{C}$ ca spațiu vectorial peste $\mathbf{R}$.

5) Ca și la pct. 4) se arată că 1 și $\sqrt{d}$ formează o bază a lui $\mathbf{Q}(\sqrt{d})$ ca spațiu vectorial peste $\mathbf{Q}$.

§ 4. PROPRIETĂȚI ALE SISTEMELOR LINIAR INDEPENDENTE (DEPENDENTE). COORDONATE

Fie V un spațiu vectorial peste corpul K și $v_1, v_2, ..., v_m \in V$. Din definiția dată sistemelor liniar independente (dependente) rezultă următoarele proprietăți:

P_1) *Dacă printre vectorii* $v_1, v_2, ..., v_m$ *se găsește vectorul* 0, *atunci sistemul de vectori* $v_1, v_2, ..., v_m$ *este liniar dependent.*

În adevăr, presupunem că $v_1 = 0$ și fie $\alpha \in K$, $\alpha \neq 0$. Atunci vectorii $v_1, v_2, ..., v_m$ verifică următoarea relație de dependență liniară nebanală

$$\alpha \cdot 0 + 0 \cdot v_2 + ... + 0 \cdot v_m = 0.$$

Acum din P_1) rezultă:

P_2) *Dacă sistemul de vectori* $v_1, v_2, ..., v_m$ *este liniar independent, atunci* $v_i \neq 0$, $1 \leqslant i \leqslant m$.

P_3) *Dacă un subsistem* S *al sistemului de vectori* $v_1, v_2, ..., v_m$ *este liniar dependent, atunci și sistemul* $v_1, v_2, ..., v_m$ *este liniar dependent* (proprietatea unui sistem de a fi liniar dependent este *ereditar ascendentă*).

În adevăr, să presupunem, pentru a nu complica notațiile, că $S = (v_1, v_2, ..., v_r)$ cu $r < m$. Cum S este sistem liniar dependent, există $\alpha_1, \alpha_2, ..., \alpha_r \in K$, nu toți nuli, astfel încît

$$\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_r v_r = 0.$$

Atunci, pentru vectorii $v_1, v_2, ..., v_r, v_{r+1}, ..., v_m$ avem relația de dependență liniară nebanală

$$\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_r v_r + 0 \cdot v_{r+1} + ... + 0 \cdot v_m = 0.$$

Acum din P_3) rezultă:

P_4) Dacă sistemul de vectori $v_1, v_2, ..., v_m$ *este liniar independent, atunci orice subsistem* S *al său este, de asemenea, liniar independent* (proprietatea unui sistem de a fi liniar independent este *ereditar descendentă*).

Următorul rezultat este util în multe demonstrații și aplicații:

4.1. *Teoremă.* **Fie V un spațiu vectorial peste corpul K și $v_1, v_2, ..., v_r$ un sistem liniar independent de vectori din V. Pentru un vector $x \in V$ următoarele afirmații sînt echivalente:**

1) Sistemul de vectori $v_1, v_2, ..., v_r, x$ este liniar dependent.

2) Vectorul x este combinație liniară de vectorii $v_1, v_2, ..., v_r$.

Demonstrație. 1) $\Rightarrow$ 2). Cum sistemul de vectori $v_1, v_2, ..., v_m, x$ este liniar dependent, există $\alpha_1, \alpha_2, ..., \alpha_r, \alpha \in K$, nu toți nuli, astfel încît

$$\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_r v_r + \alpha x = 0.$$

Avem $\alpha \neq 0$. În adevăr, dacă $\alpha = 0$, atunci din $\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_r v_r = 0$ rezultă și $\alpha_1 = \alpha_2 = ... = \alpha_r = 0$. Contradicție. Așadar $\alpha \neq 0$ și atunci putem defini

$$\beta_i = -\alpha^{-1}\alpha_i \in K, \qquad 1 \leqslant i \leqslant r.$$

Avem:

$$x = \beta_1 v_1 + \beta_2 v_2 + ... + \beta_r v_r.$$

2) $\Rightarrow$ 1) Fie $\beta_1, \beta_2, ..., \beta_r \in K$ astfel încît

$x = \beta_1 v_1 + \beta_2 v_2 + ... + \beta_r v_r$. Atunci:

$$\beta_1 v_1 + \beta_2 v_2 + ... + \beta_r v_r + (-1)x = 0$$

și cum $-1 \neq 0$, sistemul de vectori $v_1, v_2, ..., v_r, x$ este liniar dependent.

Fie $\mathbf{B} = (e_1, e_2, ..., e_n)$ o bază a spațiului vectorial V peste corpul K. Dacă $x \in V$, atunci există $\lambda_1, \lambda_2, ..., \lambda_n \in K$ astfel încît

$$x = \lambda_1 e_1 + \lambda_2 e_2 + ... + \lambda_n e_n = \sum_{i=1}^{n} \lambda_i e_i.$$

Să observăm că scalarii $\lambda_1, \lambda_2, ..., \lambda_n$ sînt unic determinați de vectorul x și baza $\mathbf{B}$. În adevăr, dacă pentru $\lambda_1', \lambda_2', ..., \lambda_n' \in K$ avem de asemenea

$$x = \lambda_1' e_1 + \lambda_2' e_2 + ... + \lambda_n' e_n = \sum_{i=1}^{n} \lambda_i' e_i,$$

atunci

$$(\lambda_1 - \lambda_1')e_1 + (\lambda_2 - \lambda_2')e_2 + ... + (\lambda_n - \lambda_n')e_n = \sum_{i=1}^{n} \lambda_i e_i - \sum_{i=1}^{n} \lambda_i' e_i = x - x = 0$$

și cum sistemul de vectori $e_1, e_2, ..., e_n$ este liniar independent, rezultă că

$$\lambda_1 - \lambda_1' = \lambda_2 - \lambda_2' = ... = \lambda_n - \lambda_n' = 0,$$

deci

$$\lambda_i = \lambda_i', \qquad 1 \leqslant i \leqslant n.$$

4.2. *Definiție.* **Fie V un spațiu vectorial peste corpul K, $\mathbf{B} = (e_1, e_2, ..., e_n)$ o bază a lui V și x un vector din V. Scalarii unic determinați $\lambda_1, \lambda_2, ..., \lambda_n \in K$ astfel încît**

$$x = \lambda_1 e_1 + \lambda_2 e_2 + ... + \lambda_n e_n$$

se numesc *coordonatele* **vectorului x în baza $\mathbf{B}$.**

Exemple

1. *Coordonate în baza canonică a lui* $\mathbf{R}^n$. În spațiul vectorial $\mathbf{R}^3$ să considerăm vectorii $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, $e_3 = (0, 0, 1)$.

Dacă $x \in \mathbf{R}^3$, $x = (a_1, a_2, a_3)$, atunci:

$$x = (a_1, 0, 0) + (0, a_2, 0) + (0, 0, a_3) = a_1(1, 0, 0) + a_2(0, 1, 0) + a_3(0, 0, 1) = a_1 e_1 + a_2 e_2 + a_3 e_3,$$

deci $\mathbf{B} = (e_1, e_2, e_3)$ este un sistem de generatori pentru $\mathbf{R}^3$.

Dacă pentru $\alpha_1, \alpha_2, \alpha_3 \in \mathbf{R}$ avem

$$\alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 = 0,$$

atunci

$$(\alpha_1, \alpha_2, \alpha_3) = (0, 0, 0),$$

de unde $\alpha_1 = \alpha_2 = \alpha_3 = 0$. Așadar sistemul de vectori $\mathbf{B}$ este și liniar independent, deci bază a spațiului vectorial $\mathbf{R}^3$, numită *baza canonică* a lui $\mathbf{R}^3$. Cum pentru orice $x \in \mathbf{R}^3$, $x = (a_1, a_2, a_3)$ avem

$$x = a_1 e_1 + a_2 e_2 + a_3 e_3,$$

rezultă că coordonatele în baza canonică a unui vector $x \in \mathbf{R}^3$ coincid cu componentele acestuia.

Să observăm că coordonatele unui vector diferă de la o bază la alta. Astfel, dacă $v = (3, -2{,}5) \in \mathbf{R}^3$, cum

$$v = 3e_1 - 2e_2 + 5e_3$$

coordonatele lui v în baza canonică a lui $\mathbf{R}^3$ sînt 3, $-2{,}5$ (= cu componentele lui v). Pe de altă parte, vectorii $v_1 = (-1, 1, 1)$, $v_2 = (1, -1, 1)$, $v_3 = (1, 1, -1)$ formează, de asemenea, o bază a lui $\mathbf{R}^3$ (v. Ex. R—1, § 3) și coordonatele lui $v = (3, -2, 5)$ în baza v_1, v_2, v_3 sînt $\frac{3}{2}$, 4, $\frac{1}{2}$ pentru că

$$v = \frac{3}{2} v_1 + 4v_2 + \frac{1}{2} v_3.$$

Analog, în spațiul vectorial $\mathbf{R}^n$ (sau chiar în K^n, K corp oarecare) vectorii

$e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, \ldots, 0)$, $\ldots$, $e_n = (0, 0, \ldots, 1)$ formează o bază a lui $\mathbf{R}^n$ (resp. K^n) numită *baza canonică* a lui $\mathbf{R}^n$ (resp. K^n). Mai mult pentru orice $x = (a_1, a_2, \ldots, a_n)$ avem

$$x = a_1 e_1 + a_2 e_2 + \ldots + a_n e_n,$$

deci coordonatele lui x în baza canonică coincid cu componentele sale, anume $a_1, a_2, \ldots, a_n$.

2. *Dezvoltarea unui polinom din $\mathbf{R}[X]$ după puterile lui $X - a$.* Fie V mulțimea tuturor polinoamelor $f \in \mathbf{R}[X]$ de grad cel mult 3. Se observă că dacă $f, g \in V$, atunci $f + g \in V$ și $-f, \in V$, deci V este subgrup al grupului $(\mathbf{R}[X], +)$. Rezultă că V este grup în raport cu operația indusă de adunarea polinoamelor.

Pe grupul abelian $(V, +)$ înmulțirea polinoamelor cu scalari determină o structură de spațiu vectorial peste $\mathbf{R}$, numit *spațiul vectorial al polinoamelor de grad $\leqslant 3$*.

Dacă $f \in V$, atunci $f = a_0 + a_1 X + a_2 X^2 + a_3 X^3$ cu $a_0, a_1, a_2, a_3 \in \mathbf{R}$. Rezultă că polinoamele $1, X, X^2, X^3$ formează un sistem de generatori pentru spațiul vectorial V.

Dacă pentru $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbf{R}$ avem

$$\alpha_0 \cdot 1 + \alpha_1 X + \alpha_2 X^2 + \alpha_3 X^3 = 0 = 0 \cdot 1 + 0 \cdot X + 0 \cdot X^2 + 0 \cdot X^3,$$

din definiția egalității polinoamelor rezultă că $\alpha_0 = \alpha_1 = \alpha_2 = \alpha_3 = 0$, deci $(1, X, X^2, X^3)$ este o bază a lui V și coordonatele oricărui polinom $f \in V$ în baza $(1, X, X^2, X^3)$ coincid cu coeficienții lui f.

Pentru orice $a \in \mathbf{R}$, polinoamele $p_i = (X - a)^i$, $0 \leqslant i \leqslant 3$, $p_0 = 1$, $p_1 = X - a$, $p_2 = (X - a)^2$, $p_3 = (X - a)^3$
formează, de asemenea, o bază a lui V. În adevăr, fie $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbf{R}$ astfel încît

$$\alpha_0 \cdot 1 + \alpha_1 (X - a) + \alpha_2 (X - a)^2 + \alpha_3 (X - a)^3 = 0.$$

Atunci

$$\alpha_0 - \alpha_1 a + \alpha_2 a^2 - \alpha_3 a^3 + (\alpha_1 - 2\alpha_2 a + 3\alpha_3 a^2) X + (\alpha_2 - 3\alpha_3 a) X^2 + \alpha_3 X^3 = 0.$$

Rezultă că

$$\begin{cases} \alpha_3 = 0, \\ \alpha_2 - 3\alpha_3 a = 0, \\ \alpha_1 - 2\alpha_2 a + 3\alpha_3 a^2 = 0, \\ \alpha_0 - \alpha_1 a + \alpha_2 a^2 - \alpha_3 a^3 = 0, \end{cases}$$

de unde $\alpha_0 = \alpha_1 = \alpha_2 = \alpha_3 = 0$, deci polinoamele p_0, p_1, p_2, p_3 sînt liniar independente peste $\mathbf{R}$. Să arătăm că polinoamele p_0, p_1, p_2, p_3 formează și un sistem de generatori pentru V. Pentru orice $f \in V$, $f = a_0 + a_1 X + a_2 X^2 + a_3 X^3$ trebuie să arătăm că există $\lambda_0, \lambda_1, \lambda_2, \lambda_3 \in \mathbf{R}$ astfel încît

(0) $$f = \lambda_0 \cdot 1 + \lambda_1 (X - a) + \lambda_2 (X - a)^2 + \lambda_3 (X - a)^3.$$

Luînd derivata formală, egalitatea precedentă devine succesiv:

(1) $$Df = \lambda_1 + 2\lambda_2 (X - a) + 3\lambda_3 (X - a)^2,$$

(2) $$D^2 f = 2!\lambda_2 + 2 \cdot 3\lambda_3 (X - a),$$

(3) $$D^3 f = 3!\lambda_3.$$

În egalitățile (0) — (3) luînd valoarea polinomului în punctul a, obtinem:

$$\lambda_0 = f(a) = a_0 + a_1 a + a_2 a^2 + a_3 a^3,$$

$$\lambda_1 = \frac{1}{1!} Df(a) = a_1 + 2a_2 a + 3a_3 a^2,$$

$$\lambda_2 = \frac{1}{2!} D^2 f(a) = a_2 + 3a_3 a,$$

$$\lambda_3 = \frac{1}{3!} D^3 f(a) = a_3,$$

deci

$$f = f(a) + \frac{1}{1!} Df(a)(X - a) + \frac{1}{2!} D^2 f(a)(X - a)^2 + \frac{1}{3!} D^3 f(a)(X - a)^3.$$

În general, dacă V este spațiul vectorial al polinoamelor $f \in \mathbf{R}[X]$ cu grad $f \leqslant n$, atunci pentru orice $a \in \mathbf{R}$, polinoamele

$$1,\ X - a,\ (X - a)^2,\ \ldots,\ (X - a)^n$$

formează o bază a lui V și coordonatele unui polinom $f \in V$ în această bază sînt

$$f(a),\quad \frac{1}{1!} Df(a),\quad \frac{1}{2!} D^2 f(a),\ \ldots,\quad \frac{1}{n!} D^n f(a),$$

deci

$$f = f(a) + \frac{1}{1!} Df(a)(X - a) + \frac{1}{2!} D^2 f(a)(X - a)^2 + \ldots +$$

$$+ \frac{1}{n!} D^n f(a)\,(X - a)^n.$$

Astfel, dacă $f = -4 + 3X - 5X^2 + 2X^3$ și $a = 2$

atunci

$$Df = 3 - 10X + 6X^2,$$

$$D^2 f = -10 + 12X,$$

$$D^3 f = 12$$

deci

$$f(2) = -2,\ Df(2) = 7,\ D^2 f(2) = 14,\ D^3 f(2) = 12,$$

de unde

$$f = f(2) + \frac{1}{1!} Df(2)(X - 2) + \frac{1}{2!} D^2 f(2)(X - 2)^2 + \frac{1}{3!} D^3 f(2)(X-2)^3 =$$

$$= -2 + 7(X - 2) + 7(X - 2)^2 + 2(X - 2)^3.$$

§ 5. LEMA SUBSTITUȚIEI

Trecerea de la o bază la alta a unui spațiu vectorial V, precum și modul în care se transformă coordonatele vectorilor cînd se face o schimbare de bază, se descrie în lema următoare, într-un caz particular foarte important.

5.1. *Lemă* **(a substituției). Fie $\mathbf{B} = (e_1, e_2, \ldots, e_n)$ o bază a unui spațiu vectorial V peste corpul K și $v \in V$, $v = \alpha_1 e_1 + \alpha_2 e_2 + \ldots + \alpha_n e_n$. Fie $\mathbf{B}^* = (e_1, e_2, \ldots, e_{i-1}, v, e_{i+1}, \ldots, e_n)$.**

1) $\mathbf{B}^*$ este bază a lui V dacă și numai dacă $\alpha_i \neq 0$.

2) Dacă $\mathbf{B}^*$ este bază a lui V, atunci coordonatele $\lambda_1^*, \lambda_2^*, \ldots, \lambda_n^*$ în baza $\mathbf{B}^*$ ale unui vector $x \in V$ se exprimă în funcție de coordonatele sale $\lambda_1, \lambda_2, \ldots, \lambda_n$ din baza $\mathbf{B}$ prin relațiile:

$$\boxed{\lambda_i^* = \lambda_i/\alpha_i,\ \lambda_j^* = \lambda_j - (\alpha_j \lambda_i)/\alpha_i \text{ pentru } j \neq i}$$

Demonstrație. Presupunem că $i = 1$ și $n = 3$. Demonstrația în cazul general este asemănătoare cu ceea ce urmează. Să arătăm că $\mathbf{B}^* = (v, e_2, e_3)$ este sistem liniar independent dacă și numai dacă $\alpha_1 \neq 0$.

Presupunem că pentru $\mu_1, \mu_2, \mu_3 \in K$ avem:

$$\mu_1 v + \mu_2 e_2 + \mu_3 e_3 = 0. \tag{1}$$

Cum $v = \alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3$, din (1) deducem:

$$\mu_1 \alpha_1 e_1 + (\mu_2 + \mu_1 \alpha_2) e_2 + (\mu_3 + \mu_1 \alpha_3) e_3 = 0$$

și cum vectorii e_1, e_2, e_3 sînt liniar independenți rezultă:

$$\begin{cases} \mu_1 \alpha_1 = 0, \\ \mu_2 + \mu_1 \alpha_2 = 0, \\ \mu_3 + \mu_1 \alpha_3 = 0. \end{cases} \tag{2}$$

Relațiile (2) constituie un sistem omogen de trei ecuații în μ_1, μ_2, μ_3. Determinantul acestui sistem este:

$$\Delta = \begin{vmatrix} \alpha_1 & 0 & 0 \\ \alpha_2 & 1 & 0 \\ \alpha_2 & 0 & 1 \end{vmatrix} = \alpha_1.$$

Se știe că sistemul (2) are numai soluția banală $\mu_1 = \mu_2 = \mu_3 = 0$ dacă și numai dacă $\Delta \neq 0$. Astfel spus, relația (1) este adevărată numai cînd $\mu_1 = \mu_2 = \mu_3 = 0$ dacă și numai dacă $\alpha_1 \neq 0$. Deci $\mathbf{B}^*$ este sistem liniar independent dacă și numai dacă $\alpha_1 \neq 0$.

Presupunem că $\alpha_1 \neq 0$ și fie $x \in V$, $x = \lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3$. Cum $\alpha_1 \neq 0$, avem:

$$e_1 = \frac{1}{\alpha_1} v - \frac{\alpha_2}{\alpha_1} e_2 - \frac{\alpha_3}{\alpha_2} e_3,$$

de unde

$$x = \lambda_1 \left(\frac{1}{\alpha_1} u - \frac{\alpha_2}{\alpha_1} e_2 - \frac{\alpha_2}{\alpha_2} e_3 \right) + \lambda_2 e_2 + \lambda_3 e_3 = \frac{\lambda_1}{\alpha_1} u + \left(\lambda_2 - \frac{\alpha_2 \lambda_1}{\alpha_1} \right) e_2 +$$

$$+ \left(\lambda_3 - \frac{\alpha_3 \lambda_1}{\alpha_1} \right) e_3.$$

Așadar, dacă $\alpha_1 \neq 0$, atunci $\mathbf{B}^* = (v, e_2, e_3)$ este și sistem de generatori al lui V, deci bază a lui V. Totodată, se obține și afirmația 2) din enunț pentru $i = 1$ și $n = 3$.

Lema substituției are un rol decisiv în elaborarea unor metode numerice remarcabile ale algebrei liniare.

Calculul tipic ce trebuie efectuat în cadrul acestor metode constă, păstrînd notațiile din lema substituției, în a găsi coordonatele în baza $\mathbf{B}^*$ ale vectorilor v, x, y, ... cînd se cunosc coordonatele acestora în baza $\mathbf{B}$. Se folosesc în acest scop tabele a căror linii corespund vectorilor bazei $\mathbf{B}$, respectiv $\mathbf{B}^*$ și în coloanele cărora sînt înserate coordonatele vectorilor v, x, y, ... în baza $\mathbf{B}$, respectiv $\mathbf{B}^*$.

	...v...	x...
e_1	α_1	λ_1
⋮	⋮	⋮
e_i	$\boxed{\alpha_i}$	λ_i
⋮	⋮	⋮
e_j	α_j	λ_j
⋮	⋮	⋮
e_n	α_n	λ_n

Tabelul $\mathbf{B}$

→

	...v...	x...
e_1	0	$\lambda_1 - (\alpha_1 \lambda_i)/\alpha_i$
⋮	⋮	⋮
v	1	λ_i/α_i
⋮	⋮	⋮
e_j	0	$\lambda_j - (\alpha_j \lambda_i)/\alpha_i$
⋮	⋮	⋮
e_n	0	$\lambda_n - (\alpha_n \lambda_i)/\alpha_i$

Tabelul $\mathbf{B}^*$

Cînd $\alpha_i \neq 0$ vectorul e_i al bazei $\mathbf{B}$ se poate înlocui cu vectorul v și se obține baza $\mathbf{B}^*$. În acest caz α_i din Tabelul $\mathbf{B}$ este declarat *pivot* și se încadrează într-un pătrat. Acum Tabelul $\mathbf{B}^*$ se obține din Tabelul $\mathbf{B}$ după cum urmează:

a) *se împart la pivot toate elementele din linia acestuia*;

b) *pivotul se înlocuiește cu 1 și celelalte elemente din coloana acestuia se înlocuiesc cu* 0;

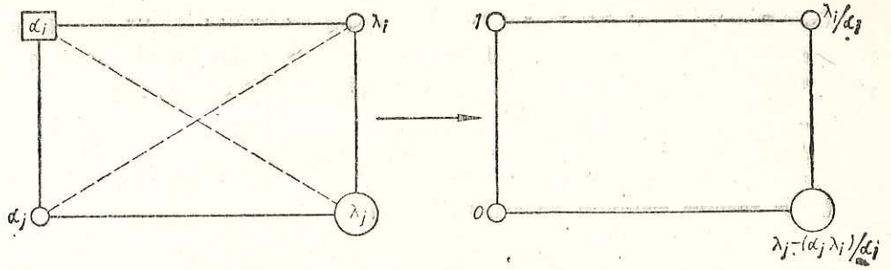


Fig. VI.3

c) *toate elementele* λ_j *din afara liniei și coloanei pivotului se înlocuiesc cu* $\lambda_j - (\alpha_j \lambda_i)/\alpha_i$, *operație cunoscută sub numele de „regula dreptunghiului"* (v. Fig. VI.3)

Aplicații ale lemei substituției

A—1 *Testul bazei; calculul coordonatelor*

În spațiul vectorilor coloană $\mathbf{R}^3$ considerăm vectorii

$$v_1 = \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}, \quad v_3 = \begin{pmatrix} -1 \\ -1 \\ -2 \end{pmatrix}, \quad v = \begin{pmatrix} 1 \\ -1 \\ -2 \end{pmatrix}.$$

Folosind lema substituției, să arătăm că vectorii v_1, v_2, v_3 formează o bază a lui $\mathbf{R}^3$ și să găsim coordonatele lui v în această bază.

Fie $\mathbf{B} = (e_1, e_2, e_3)$ baza canonică a lui $\mathbf{R}^3$,

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Avem: $v_1 = 2e_1 + e_2 + e_3$, $v_2 = 3e_1 + 2e_2 + e_3$, $v_3 = -e_1 - e_2 - 2e_3$, și $v = e_1 - e_2 - 2e_3$. Vom încerca să înlocuim vectorii bazei $\mathbf{B}$ succesiv cu vectorii v_1, v_2, v_3 și vom face de fiecare dată calculul coordonatelor vectorilor v_1, v_2, v_3 și v conform lemei substituției. Primul tabel corespunde bazei $\mathbf{B}$. Avem:

	v_1	v_2	v_3	v
e_1	$\boxed{2}$	3	−1	1
e_2	1	2	−1	−1
e_3	1	1	−2	−2

→

	v_1	v_2	v_3	v
v_1	1	3/2	−1/2	1/2
e_2	0	$\boxed{1/2}$	−1/2	−3/2
e_3	0	−1/2	−3/2	−5/2

→

	v_1	v_2	v_3	v
v_1	1	0	1	5
v_2	0	1	−1	−3
e_3	0	0	$\boxed{-2}$	−4

→

	v_1	v_2	v_3	v
v_1	1	0	0	3
v_2	0	1	0	−1
v_3	0	0	1	2

Cum $\mathbf{B} = (e_1, e_2, e_3)$ este bază a lui $\mathbf{R}^3$, din lema substituției rezultă succesiv că (v_1, e_2, e_3), (v_1, v_2, e_3) și (v_1, v_2, v_3) sînt baze ale lui $\mathbf{R}^3$. În ultima coloană din ultimul tabel sînt conținute coordonatele lui v în baza (v_1, v_2, v_3), deci $v = 3v_1 - v_2 + 2v_3$.

A—2 *Rezolvarea sistemelor de ecuații liniare.*

Să se rezolve sistemul de ecuații liniare

$$(S)\begin{cases} 2x_1 + 3x_2 - x_3 = 1, \\ x_1 + 2x_2 - x_3 = -1, \\ x_1 + x_2 - 2x_3 = -2. \end{cases}$$

Fie A matricea sistemului (S) și L vectorul coloană al termenilor liberi,

$$A = \begin{pmatrix} 2 & 3 & -1 \\ 1 & 2 & -1 \\ 1 & 1 & -2 \end{pmatrix}, \quad L = \begin{pmatrix} 1 \\ -1 \\ -2 \end{pmatrix}.$$

Să notăm cu c_1^A, c_2^A, c_3^A coloanele matricei A,

$$c_1^A = \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}, \quad c_2^A = \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}, \quad c_3^A = \begin{pmatrix} -1 \\ -1 \\ -2 \end{pmatrix}$$

și să observăm că avem:

$$c_1^A x_1 + c_2^A x_2 + c_3^A x_3 = \begin{pmatrix} 2x_1 + 3x_2 - x_3 \\ x_1 + 2x_2 - x_3 \\ x_1 + x_2 - 2x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \\ -2 \end{pmatrix} = L.$$

Așadar, scalarii α_1, α_2, α_3 formează o soluție a sistemului (S) dacă și numai dacă

$$c_1^A \alpha_1 + c_2^A \alpha_2 + c_3^A \alpha_3 = L.$$

Observînd că $c_1^A = v_1$, $c_2^A = v_2$, $c_3^A = v_3$ și $L = v$, unde v_1, v_2, v_3 și v sînt vectorii de la $A - 1$, rezultă, folosind calculul făcut la $A - 1$ cu lema substituției, că sistemul (S) este compatibil și admite soluție unică, anume $x_1 = 3$, $x_2 = -1$, $x_3 = 2$.

A—3 *Calculul inversei unei matrice.*

Fie A, B, $E \in M_3(\mathbf{R})$,

$$A = \begin{pmatrix} 2 & 3 & -1 \\ 1 & 2 & -1 \\ 1 & 1 & -2 \end{pmatrix}, \quad B = \begin{pmatrix} x & x' & x'' \\ y & y' & y'' \\ z & z' & z'' \end{pmatrix}, \quad E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Să determinăm matricea B astfel încît $AB = E$.

Din egalitatea $AB = E$ deducem:

$$\left(\begin{array}{ccc|ccc} 2x + 3y - z & 2x' + 3y' - z' & 2x'' + 3y'' - z'' \\ x + 2y - z & x' + 2y'' - z' & x'' + 2y'' - z'' \\ x + y - 2z & x' + y' - 2z' & x'' + y'' - 2z'' \end{array}\right) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

ceea ce este echivalent cu următoarele trei sisteme de ecuații liniare:

$$(S)\begin{cases} 2x + 3y - z = 1, \\ x + 2y - z = 0, \\ x + y - 2z = 0; \end{cases} \quad (S')\begin{cases} 2x' + 3y' - z' = 0, \\ x' + 2y' - z' = 1, \\ x' + y' - 2z' = 0; \end{cases} \quad (S'')\begin{cases} 2x'' + 3y'' - z'' = 0, \\ x'' + 2y'' - z'' = 0, \\ x'' + y'' - 2z'' = 1. \end{cases}$$

Sistemele (S), (S') și (S'') se mai pot scrie

$$(S) \quad c_1^A x + c_2^A y + c_3^A z = e_1,$$

$$(S') \quad c_1^A x' + c_2^A y' + c_3^A z' = e_2,$$

$$(S'') \quad c_1^A x'' + c_2^A y'' + c_3^A z'' = e_3,$$

unde e_1, e_2, e_3 sînt vectorii bazei canonice a spațiului vectorilor coloană $\mathbf{R}^3$. Cum matricea fiecăruia din sistemele (S), (S') și (S'') este egală cu A, putem da o rezolvare simultană a lor cu următoarea organizare a calculelor pe baza lemei substituției:

	c_1^A	c_2^A	c_3^A	e_1	e_2	e_3
e_1	[2]	3	−1	1	0	0
e_2	1	2	−1	0	1	0
e_3	1	1	−2	0	0	1

→

	c_1^A	c_2^A	c_3^A	e_1	e_2	e_3
c_1^A	1	3/2	−1/2	1/2	0	0
e_2	0	[1/2]	−1/2	−1/2	1	0
e_3	0	−1/2	−3/2	−1/2	0	1

→

	c_1^A	c_2^A	c_3^A	e_1	e_2	e_3
c_1^A	1	0	1	2	−3	0
c_2^A	0	1	−1	−1	2	0
e_3	0	0	[−2]	−1	1	1

→

	c_1^A	c_2^A	c_3^A	e_1	e_2	e_3
c_1^A	1	0	0	3/2	−5/2	1/2
c_2^A	0	1	0	−1/2	3/2	−1/2
c_3^A	0	0	1	1/2	−1/2	−1/2.

În al doilea compartiment din ultimul tabel se găsește matricea căutată B,

$$B = \begin{pmatrix} 3/2 & -5/2 & 1/2 \\ -1/2 & 3/2 & -1/2 \\ 1/2 & -1/2 & -1/2 \end{pmatrix} = A^{-1}.$$

A—4 *Determinarea unui subsistem maximal liniar independent.*

În spațiul vectorilor coloană $\mathbf{R}^3$ considerăm vectorii:

$$v_1 = \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 2 \\ 4 \\ -2 \end{pmatrix}, \quad v_3 = \begin{pmatrix} -1 \\ 0 \\ 2 \end{pmatrix}, \quad v_4 = \begin{pmatrix} 2 \\ 6 \\ -1 \end{pmatrix}.$$

Să determinăm un *subsistem maximal liniar independent* al sistemului de vectori v_1, v_2, v_3, v_4, adică o parte S a mulțimii $\{v_1, v_2, v_3, v_4\}$ formată cu vectori liniari independenți și care să nu poată fi inclusă strict într-o altă parte a lui $\{v_1, v_2, v_3, v_4\}$ formată tot cu vectori liniar independenți.

Folosind lema substituției, facem calculul următor:

	v_1	v_2	v_3	v_4
e_1	[1]	2	−1	2
e_2	2	4	0	6
e_3	−1	−2	2	−1

→

	v_1	v_2	v_3	v_4
v_1	1	2	−1	2
e_2	0	0	[2]	2
e_3	0	0	1	1

→

	v_1	v_2	v_3	v_4
v_1	1	2	0	3
v_3	0	0	1	1
e_3	0	0	0	0.

Cum (e_1, e_2, e_3) este bază a lui $\mathbf{R}^3$, din lema substituției rezultă că (v_1, e_2, e_3) și (v_1, v_3, e_3) sînt baze ale lui $\mathbf{R}^3$. Atunci (v_1, v_3) este sistem liniar independent ca parte a sistemului liniar independent (v_1, v_3, e_3) (v. P_4, § 4). Din ultimul tabel mai rezultă că v_2 și v_4 sînt combinații liniare de vectorii sistemului (v_1, v_3), anume:

$$v_2 = 2v_1 + 0 \cdot v_3 + 0e_3 = 2v_1 + 0 \cdot v_3,$$

$$v_4 = 3v_1 + v_3 + 0 \cdot e_3 = 3v_1 + v_3.$$

Aplicînd Teorema 4.1 rezultă că (v_1, v_3) este subsistem maximal liniar independent.

În tabelul al doilea putem introduce în bază vectorul v_4 în loc de v_2. Dacă alegem o asemenea cale se obține în final subsistemul maximal liniar independent (v_1, v_4).

A—5 *Dezvoltarea unui polinom după puterile lui* $X - a$.

Fie $f \in \mathbf{R}[X]$, $f = -4 + 3X - 5X^2 + 2X^3$. Să dezvoltăm polinomul f după puterile lui $X - 2$ (v. Exp. 2, § 4).

Dacă V este spațiul vectorial al polinomului de grad $\leqslant 3$ știm că $1, X, X^2, X^3$ și $1, X-2, (X-2)^2, (X-2)^3$ sînt baze ale lui V (v. Exp. 2, § 4). Pentru a obține rezultatul dorit facem următorul calcul cu lema substituției:

	1	$X-2$	$(X-2)^2$	$(X-2)^3$	f
1	1	−2	4	−8	−4
X	0	1	−4	12	3
X^2	0	0	1	−6	−5
X^3	0	0	0	[1]	2

→

	1	$X-2$	$(X-2)^2$	$(X-2)^3$	f
1	1	−2	4	0	12
X	0	1	−4	0	−21
X^2	0	0	[1]	0	7
$(X-1)^3$	0	0	0	1	2

↪

	1	$X-2$	$(X-2)^2$	$(X-2)^3$	f
1	1	−2	0	0	−16
X	0	[1]	0	0	7
$(X-2)^2$	0	0	1	0	7
$(X-2)^3$	0	0	0	1	2

→

	1	$X-2$	$(X-2)^2$	$(X-2)^3$	f
1	1	0	0	0	−2
$X-2$	0	1	0	0	7
$(X-2)^2$	0	0	1	0	7
$(X-2)^3$	0	0	0	1	2

Din ultimul tabel obținem

$$f = -2 + 7(X-2) + 7(X-2)^2 + 2(X-2)^3,$$

rezultat ce coincide cu cel de la Exp. 2, § 4 obținut pe altă cale.

Observație. Schema lui Horner permite calculul valorii $f(a)$; cu lema substituției se realizează calculul simultan al valorilor $f(a)$, $Df(a)$, ..., $D^n f(a)$.

§ 6. TRANSFORMĂRI LINIARE

În capitolele anterioare au fost definite și studiate morfismele de grupuri (inele, corpuri). Acestea sînt aplicații între două grupuri (resp. inele, corpuri) cu proprietatea definitorie că luarea imaginilor elementelor comută cu compunerea lor. În același spirit, pentru spații vectoriale se introduce noțiunea următoare:

6.1. *Definiție.* **Fie V și V' două spații vectoriale peste un același corp K. O aplicație $f : V \to V'$ se numește *transformare liniară* dacă:**

1) $f(x + y) = f(x) + f(y)$, $\quad \forall\, x, y \in V$;

2) $f(\alpha x) = \alpha f(x)$ $\quad \forall\, \alpha \in K,\ x \in V$.

Dacă $f : V \to V'$ este o transformare liniară, din 1) rezultă că f este, în particular, morfism de la grupul $(V, +)$ la grupul $(V', +)$. Aplicînd Teorema 6.4. Cap. III, deducem:

$$\boxed{f(0) = 0', \quad f(-x) = -f(x),\ \forall\, x \in V}$$

unde 0 este vectorul zero al lui V și $0'$ este vectorul zero al lui V'.

De asemenea:

$$\boxed{f\left(\sum_{i=1}^{n} \alpha_i x_i\right) = \sum_{i=1}^{n} \alpha_i f(x_i) \qquad \forall\, \alpha_i \in K,\ x_i \in V,\ n \geqslant 1}.$$

În adevăr, dacă $n = 1$ proprietatea rezultă din 2). Dacă $n > 1$, atunci presupunînd proprietatea adevărată pentru $n - 1$, avem:

$$f\left(\sum_{i=1}^{n} \alpha_i x_i\right) = f\left(\sum_{i=1}^{n-1} \alpha_i x_i + x_n\right) = f\left(\sum_{i=1}^{n-1} \alpha_i x_i\right) + f(x_n) =$$

$$= \sum_{i=1}^{n-1} \alpha_i f(x_i) + f(x_n) = \sum_{i=1}^{n} \alpha_i f(x_i).$$

Dacă $V = V'$, atunci f se numește *transformare liniară* sau *endomorfism* al lui V. Se notează cu $\mathrm{End}_K V$ mulțimea tuturor transformărilor liniare ale lui V.

Exemple

1. Fie $V = \mathbf{R}^2$ și $A \in M_2(\mathbf{R})$, $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$.

Atunci aplicația $f_A : V \to V$,

$$f_A(x) = (a_{11}x_1 + a_{12}x_2,\ a_{21}x_1 + a_{22}x_2), \qquad \forall\, x = (x_1,\ x_2) \in \mathbf{R}^2$$

este o transformare liniară a spațiului vectorial $\mathbf{R}^2$.

În adevăr, dacă $\alpha \in \mathbf{R}$ și $x, y \in \mathbf{R}^2$, $x = (x_1, x_2)$, $y = (y_1, y_2)$, atunci

$$x + y = (x_1 + y_1,\ x_2 + y_2),$$
$$\alpha x = (\alpha x_1,\ \alpha x_2),$$

de unde

$$f_A(x + y) = (a_{11}(x_1 + y_1) + a_{12}(x_2 + y_2),\ a_{21}(x_1 + y_1) + a_{22}(x_2 + y_2)) =$$
$$= (a_{11}x_1 + a_{11}y_1 + a_{12}x_2 + a_{12}y_2,\ a_{21}x_1 + a_{21}y_1 + a_{22}x_2 + a_{22}y_2) =$$
$$= (a_{11}x_1 + a_{12}x_2,\ a_{21}x_1 + a_{22}x_2) + (a_{11}y_1 + a_{12}y_2,\ a_{21}y_1 + a_{22}y_2) =$$
$$= f_A(x) + f_A(y)$$

și

$$f_A(\alpha x) = (a_{11}(\alpha x_1) + a_{12}(\alpha x_2),\ a_{21}(\alpha x_1) + a_{22}(\alpha x_2)) =$$
$$= \alpha(a_{11}x_1 + a_{12}x_2,\ a_{21}x_1 + a_{22}x_2) = \alpha f_A(x).$$

2. Aplicația $f : \mathbf{R}^2 \to \mathbf{R}^2$,

$$f(x) = (2x_1 + 3x_2,\ x_1 + x_2 + 1), \quad \forall\, x = (x_1,\ x_2) \in \mathbf{R}^2$$

nu este transformare liniară a spațiului vectorial $\mathbf{R}^2$. În adevăr, avem, de exemplu,

$$f(3x) = (6x_1 + 9x_2,\ 3x_1 + 3x_2 + 1) = 3(2x_1 + 3x_2,\ x_1 + x_2 + 1) +$$
$$+ (0,\ -2) = 3f(x) + (0,\ -2) \neq 3f(x).$$

3. Fie V un spațiu vectorial peste corpul K și $1_V : V \to V$ aplicația identică a mulțimii V.

Cum

$$1_V(x + y) = x + y = 1_V(x) + 1_V(y), \qquad \forall x,\ y \in V$$

și

$$1_V(\alpha x) = \alpha x = \alpha 1_V(x), \qquad \forall \alpha \in K,\ x \in V,$$

rezultă că 1_V este transformare liniară a lui V, numită *transformarea identică* a lui V.

De asemenea, aplicația $0 : V \to V$, $0(x) = 0$, $\forall\, x \in V$ este transformare liniară, numită *transformarea zero* a lui V. În adevăr,

$$0(x + y) = 0 = 0 + 0 = 0(x) + 0(y), \qquad \forall x,\ y \in V$$
$$0(\alpha x) = 0 = \alpha 0 = \alpha 0(x), \qquad \forall \alpha \in K,\ x \in V.$$

4. Fie $\mathbf{R}[X]$ spațiul vectorial al polinoamelor cu coeficienți reali. Dacă $f \in \mathbf{R}[X]$, $f = a_0 + a_1X + \ldots + a_nX^n$, fie $\mathrm{D}f = a_1 + 2a_2X + \ldots + n\,a_{n-1}X^{n-1}$ derivata formală a lui f. Aplicația $\varphi : \mathbf{R}[X] \to \mathbf{R}[X]$,

$$\varphi(f) = \mathrm{D}f, \qquad \forall\, f \in \mathbf{R}[X]$$

este o transformare liniară. În adevăr,

$$\varphi(f + g) = \mathrm{D}(f + g) = \mathrm{D}f + \mathrm{D}g = \varphi(f) + \varphi(g), \qquad \forall\, f,\ g \in \mathbf{R}[X]$$
$$\varphi(\alpha f) = \mathrm{D}(\alpha f) = \alpha \mathrm{D}f = \alpha\varphi(f), \qquad \forall\, \alpha \in \mathbf{R},\ f \in \mathbf{R}[X].$$

5. Fie $\mathbf{R}^3$ și $\mathbf{R}^2$ spațiul vectorilor coloană 3-dimensionali, respectiv 2-dimensionali și matricea $A = \begin{pmatrix} -2 & 3 & 1 \\ 2 & -1 & 4 \end{pmatrix}$. Atunci aplicația $f : \mathbf{R}^3 \to \mathbf{R}^2$,

$$f(x) = A\,x = \begin{pmatrix} -2x_1 + 3x_2 + x_3 \\ 2x_1 - x_2 + 4x_3 \end{pmatrix}, \quad \forall\, x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbf{R}^3$$

este o transformare liniară.

Exerciții

1. Verificați proprietățile S_1, S_2 și S_4 pentru înmulțirea matricelor cu scalari.

2. Verificați proprietățile S_2, S_3 și S_4 pentru înmulțirea polinoamelor cu scalari.

3. Fie M o mulțime nevidă și $\mathcal{F}(M)$ mulțimea tuturor funcțiilor $f : M \to M$. Pe M definim legea de compoziție externă cu operatori în $\mathcal{F}(M)$,

$$\mathcal{F}(M) \times M \to M, \quad (f,\ x) \to f * x \overset{\text{def}}{=} f(x) \in M.$$

Arătați că:

1) $f * (g * x) = (f \circ g) * x$, $\forall\, f,\ g \in \mathcal{F}(M)$, $x \in M$;

2) $1_M * x = x$, $\forall\, x \in M$.

4. Fie $V = \mathbf{R}_+^* = \{x \in \mathbf{R} \mid x > 0\}$. Arătați că V este spațiu vectorial peste corpul $\mathbf{R}$ în raport cu legile de compoziție.

$$x \perp y \overset{\text{def}}{=} xy, \qquad \alpha \top x \overset{\text{def}}{=} x^\alpha, \qquad \forall\, \alpha \in \mathbf{R},\ x \in V.$$

5. Fie V mulțimea tuturor șirurilor f de numere reale,

$$f = (a_0, a_1, \ldots, a_n, \ldots), \qquad (a_i \in \mathbf{R}).$$

Dacă $\alpha \in \mathbf{R}$ și $f, g \in V$, $f = (a_0, a_1, \ldots, a_n, \ldots)$, $g = (b_0, b_1, \ldots, b_n, \ldots)$ atunci punem

$$f + g \overset{\text{def}}{=} (a_0 + b_0,\ a_1 + b_1, \ldots, a_n + b_n, \ldots)$$

$$\alpha f \overset{\text{def}}{=} (\alpha a_0,\ \alpha a_1, \ldots, \alpha a_n, \ldots).$$

Arătați că V este spațiu vectorial peste corpul $\mathbf{R}$ în raport cu legile de compoziție:

$$V \times V \to V, \qquad (f, g) \to f + g$$

$$\mathbf{R} \times V \to V, \qquad (\alpha, f) \to \alpha f.$$

6. Fie $K = \mathbf{Z}_2 = \{\hat{0}, \hat{1}\}$. Enumerați toți vectorii spațiului vectorial K^3. Care este numărul vectorilor spațiului vectorial K^n?

7. Arătați că pentru oricare două numere naturale p, n, cu p prim, există un spațiu vectorial V cu p^n vectori.

8. Fie $V \neq 0$ un spațiu vectorial peste corpul $\mathbf{R}$. Arătați că V are o infinitate de vectori.

9. Fie V un spațiu vectorial peste corpul $\mathbf{Z}_p$, p număr prim. Arătați că

$$0 = x + x + \ldots + x (p \text{ ori}), \qquad \forall\, x \in V.$$

10. Fie V un spațiu vectorial peste corpul K. Demonstrați prin inducție că

$$\alpha(v_1 + v_2 + \ldots + v_n) = \alpha v_1 + \alpha v_2 + \ldots + \alpha v_n$$

și

$$(\alpha_1 + \alpha_2 + \ldots + \alpha_m)v = \alpha_1 v + \alpha_2 v + \ldots + \alpha_m v$$

oricare ar fi $\alpha,\ \alpha_1, \ldots, \alpha_m \in K,\ v, v_1, \ldots, v_n \in V$.

11. Fie vectorii $v_1 = (1, 1, 0)$, $v_2 = (0, 1, 1)$, $v_3 = (1, 0, 1)$ din spațiul vectorial $\mathbf{R}^3$.

1) Arătați că sistemul de vectori $\mathbf{B} = (v_1, v_2, v_3)$ este o bază a lui $\mathbf{R}^3$.

2) Reprezentați vectorul $v = (2, -3, 5)$ ca o combinație liniară de vectorii bazei $\mathbf{B}$.

12. În spațiul vectorial $V = M_2(\mathbf{R})$ se consideră matricele

$$E_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \quad E_3 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad E_4 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} -2 & 3 \\ 4 & -2 \end{pmatrix}.$$

1) Arătați că $\mathbf{B} = (E_1, E_2, E_3, E_4)$ este o bază a lui V.

2) Reprezentați matricea A ca o combinație liniară de vectorii bazei $\mathbf{B}$.

13. Fie $f_1, f_2, f_3 \in \mathbf{R}[X]$, $f_1 = (X - b)(X - c)$, $f_2 = (X - c)(X - a)$, $f_3 = (X - a)(X - b)$

1) Arătați că polinoamele f_1, f_2, f_3 sînt liniar independente peste $\mathbf{R}$ dacă și numai dacă $(a - b)(b - c)(c - a) \neq 0$.

2) Arătați că pentru orice polinom $f \in \mathbf{R}[X]$ cu $\operatorname{grad} f \leqslant 2$, există $\lambda_1, \lambda_2, \lambda_3 \in \mathbf{R}$ unic determinați astfel încît

$$f = \lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3.$$

3) Determinați λ_1, λ_2 și λ_3 cînd $f = 1 + 2X - X^2$, $a = 1$, $b = 2$, $c = 3$.

14. Arătați că fiecare din sistemele de polinoame din $\mathbf{R}[X]$,

$$\mathbf{B} = (1, X, X^2, X^3),$$
$$\mathbf{B}' = (1 + X^2, X + X^2, X^2, X^3 + X^2),$$
$$\mathbf{B}'' = (1, X - 1), (X - 1)^2/2!, (X - 1)^3/3!)$$

sînt liniar independente peste $\mathbf{R}$ și reprezentați polinomul $f = X^3 - X^2 - X + 1$ ca o combinație liniară cu coeficienți din $\mathbf{R}$ de polinoamele din $\mathbf{B}$ (resp. $\mathbf{B}'$, $\mathbf{B}''$).

15. Fie V un spațiu vectorial peste corpul K și v_1, v_2, v_3 un sistem de vectori liniar independenți. Arătați că vectorii $v_1 + v_2$, $v_2 + v_3$, $v_3 + v_1$ sînt, de asemenea, liniar independenți.

16. Fie v_1, v_2, v_3 un sistem de vectori dintr-un spațiu vectorial V peste corpul K. Arătați că aplicația

$$f : K^3 \to V, \quad f(x) = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 \qquad \forall\, x = (\lambda_1, \lambda_2, \lambda_3) \in \mathbf{R}$$

este injectivă (surjectivă, bijectivă) dacă și numai dacă v_1, v_2, v_3 este sistem liniar independent (resp. sistem de generatori ai lui V, bază a lui V). Generalizare.

17. În spațiul vectorilor coloană $\mathbf{R}^3$ considerăm vectorii

$$v_1 = \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}, \quad v = \begin{pmatrix} 4 \\ 9 \\ -6 \end{pmatrix}, \quad w = \begin{pmatrix} 1 \\ 8 \\ -5 \end{pmatrix}.$$

Folosind lema substituției să se arate că v_1, v_2, v_3, v_4 formează o bază a lui $\mathbf{R}^3$. Găsiți coordonatele vectorilor v și w în această bază.

18. În spațiul vectorilor coloană $\mathbf{R}^4$ considerăm vectorii

$$v_1 = \begin{bmatrix} -1 \\ 2 \\ 2 \\ 2 \end{bmatrix}, \quad v_2 = \begin{bmatrix} 2 \\ -1 \\ 2 \\ 2 \end{bmatrix}, \quad v_3 = \begin{bmatrix} 2 \\ 2 \\ -1 \\ 2 \end{bmatrix}, \quad v_4 = \begin{bmatrix} 2 \\ 2 \\ 2 \\ -1 \end{bmatrix}, \quad v = \begin{bmatrix} -6 \\ 9 \\ 6 \\ -9 \end{bmatrix}.$$

Folosind lema substituției, arătați că vectorii v_1, v_2, v_3, v_4, formează o bază a lui $\mathbf{R}^4$. Găsiți coordonatele vectorului v în această bază.

19. În spațiul K^3, unde $K = \mathbf{Z}_5$, considerăm vectorii:

$$v_1 = \begin{bmatrix} \hat{2} \\ \hat{3} \\ \hat{1} \end{bmatrix}, \quad v_2 = \begin{bmatrix} \hat{1} \\ \hat{2} \\ \hat{4} \end{bmatrix}, \quad v_3 = \begin{bmatrix} \hat{0} \\ \hat{1} \\ \hat{1} \end{bmatrix}, \quad v = \begin{bmatrix} \hat{4} \\ \hat{2} \\ \hat{1} \end{bmatrix}.$$

Folosind lema substituției, arătați că v_1, v_2, v_3 este o bază a lui K^3 și găsiți coordonatele lui v în această bază.

20. Folosind lema substituției, rezolvați următoarele sisteme de ecuații liniare:

$$1)\ \begin{cases} 2x_1 - 3x_2 + x_3 = 2, \\ x_1 + 5x_2 - 4x_3 = -5; \\ 4x_1 + x_2 - 3x_3 = -4; \end{cases} \qquad 2)\ \begin{cases} x_1 + 2x_2 + x_3 + 2x_4 = 1, \\ 2x_1 + 2x_3 + x_4 = 0, \\ x_1 + 2x_2 + x_4 = 0, \\ 2x_1 + x_2 + 2x_3 + x_4 = -1. \end{cases}$$

21. Fie $A, B \in M_3(\mathbf{R})$,

$$A = \begin{pmatrix} 1 & 2 & -1 \\ 2 & 1 & 2 \\ -1 & 1 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} -2 & 1 & 1 \\ 3 & 2 & -2 \\ 1 & 2 & -1 \end{pmatrix}, \qquad C = \begin{pmatrix} 1 & 2 & 1 \\ 3 & 1 & 2 \\ 2 & 1 & 2 \end{pmatrix}.$$

Folosind lema substituției, găsiți $X, Y, Z \in M_3(\mathbf{R})$ astfel încît $AX = E$, $BY = E$, $CZ = E$, unde E este matricea unitate.

22. Fie $A, B \in M_3(\mathbf{Z}_3)$,

$$B = \begin{pmatrix} \hat{2} & \hat{0} & \hat{1} \\ \hat{1} & \hat{2} & \hat{1} \\ \hat{2} & \hat{1} & \hat{1} \end{pmatrix}, \qquad C = \begin{pmatrix} \hat{1} & \hat{1} & \hat{0} \\ \hat{0} & \hat{1} & \hat{1} \\ \hat{1} & \hat{0} & \hat{1} \end{pmatrix}.$$

Folosind lema substituției, găsiți $X, Y \in M_3(\mathbf{Z}_3)$ astfel încît $AX = E$, $BX = E$, unde E este matricea unitate din $M_3(\mathbf{Z}_3)$.

23. În spațiul vectorilor coloană $\mathbf{R}^3$ considerăm vectorii

$$v_1 = \begin{pmatrix} 1 \\ -2 \\ 3 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 2 \\ -1 \\ 2 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}, \quad v_4 = \begin{pmatrix} 4 \\ -2 \\ 4 \end{pmatrix}.$$

Găsiți un subsistem maximal liniar independent al sistemului de vectori v_1, v_2, v_3, v_4.

24. În spațiul vectorilor coloană K^3, unde $K = \mathbf{Z}_3$, considerăm vectorii

$$v_1 = \begin{pmatrix} \hat{2} \\ \hat{1} \\ \hat{0} \end{pmatrix}, \quad v_2 = \begin{pmatrix} \hat{2} \\ \hat{2} \\ \hat{1} \end{pmatrix}, \quad v_3 = \begin{pmatrix} \hat{0} \\ \hat{1} \\ \hat{1} \end{pmatrix}, \quad v_4 = \begin{pmatrix} \hat{2} \\ \hat{0} \\ \hat{2} \end{pmatrix} \quad v_5 = \begin{pmatrix} \hat{1} \\ \hat{0} \\ \hat{1} \end{pmatrix}.$$

Găsiți un subsistem maximal liniar independent al sistemului de vectori v_1, v_2, v_3, v_4, v_5.

25. Folosind lema substituției, să se dezvolte polinomul f după puterile lui $X - a$ cînd

1) $f = X^3 - 3X^2 - 4X + 10 \in \mathbf{R}[X]$, $a = 3$,

2) $f = X^3 + \hat{2}X^2 + \hat{4}X + \hat{3} \in \mathbf{Z}_5[X]$, $a = \hat{2}$.

26. Fie $f : \mathbf{R}^2 \to \mathbf{R}^2$,

$$f(x) = \left(-\frac{1}{2} x_1 - \frac{\sqrt{3}}{2} x_2, \ \frac{\sqrt{3}}{2} x_1 - \frac{1}{2} x_2 \right), \qquad \forall x = (x_1, x_2) \in \mathbf{R}^2.$$

1) Arătați că f este transformare liniară a spațiului vectorial $\mathbf{R}^2$.
2) Calculați $f^2 = f \circ f$ și $f^3 = f^2 \circ f$.

27. Fie $A \in M_2(\mathbf{R})$, $A = \begin{pmatrix} -7 & 10 \\ -5 & 8 \end{pmatrix}$ și $f_A : \mathbf{R}^2 \to \mathbf{R}^2$,

$$f_A(x) = (-7x_1 + 10x_2, \ -5x_1 + 8x_2), \quad \forall x = (x_1, x_2) \in \mathbf{R}^2.$$

1) Arătați că f_A este transformare liniară a lui $\mathbf{R}^2$.
2) Pentru ce valori $\lambda \in \mathbf{R}$ există $x \in \mathbf{R}^2$, $x \neq 0$ astfel încît $f(x) = \lambda x$?
3) Dacă pentru $\lambda, \mu \in \mathbf{R}$ și $x, y \in \mathbf{R}^2$, $\lambda \neq \mu$, $x \neq 0$, $y \neq 0$ avem $f_A(x) = \lambda x$ și $f_A(y) = \mu y$, atunci vectorii x, y sînt liniar independenți.

* * *

28.* Considerînd pe $\mathbf{R}$ ca spațiu vectorial peste $\mathbf{Q}$ (v. Ex. R-2, § 3) arătați că $1, \sqrt[3]{2}$ și $\sqrt[3]{4}$ sînt liniar independenți peste $\mathbf{Q}$.

29.* Fie $v, v', v'' \in \mathbf{R}^3$, $v = (a, b, c)$, $v' = (a', b', c')$, $v'' = (a'', b'', c'')$.

1) Arătați că sistemul de vectori v, v', v'' este liniar independent dacă și numai dacă

$$\begin{vmatrix} a & a' & a'' \\ b & b' & b'' \\ c & c' & c'' \end{vmatrix} \neq 0.$$

2) Deduceți că orice sistem liniar independent format cu trei vectori v, v', v'' din $\mathbf{R}^3$ este o bază a spațiului vectorial $\mathbf{R}^3$. Generalizare.

30.* Fie $S = (v_1, v_2, \ldots, v_m)$ un sistem de generatori ai unui spațiu vectorial V. Arătați că orice subsistem maximal liniar independent $\mathbf{B}$ al lui S este bază a lui V.

31.* Fie V un spațiu vectorial peste corpul K, $\mathbf{B} = (e_1, e_2, \ldots, e_n)$ o bază a lui V și $v_1, v_2, \ldots, v_n$ un sistem de vectori din V liniar independenți.

1) (teorema schimbului) Arătați că $r \leqslant n$ și că r vectori din $\mathbf{B}$ pot fi înlocuiți cu $v_1, v_2, \ldots, v_r$ astfel încît ceea ce se obține să fie tot o bază a lui V.

2) (teorema bazei) Orice bază a lui V conține n vectori.

32.* Pentru un spațiu vectorial V peste K următoarele afirmații sînt echivalente:

1) V admite o bază cu n vectori.
2) Numărul maxim de vectori liniar independenți este egal cu n.

33.* Fie V un spațiu vectorial care admite o bază cu n vectori. Pentru un sistem de vectori $v_1, v_2, \ldots, v_n$ din V următoarele afirmații sînt echivalente *(teorema alternativă)*:

1) Sistemul $v_1, v_2, \ldots, v_n$ este bază a lui V;
2) $v_1, v_2, \ldots, v_n$ este un sistem de generatori al lui V;
3) Sistemul $v_1, v_2, \ldots, v_n$ este liniar independent.

34.* Arătați că proprietatea de comutativitate a adunării vectorilor este o consecință a celorlalte axiome ale spațiului vectorial.

35.* Fie $f_1, f_2, \ldots, f_n$ polinoame diferite de 0 din $\mathbf{R}[X]$ astfel încît grad $f_i \neq$ grad f_j pentru $i \neq j$.

1) Arătați că polinoamele $f_1, f_2, \ldots, f_n$ sînt liniar independente peste $\mathbf{R}$.

2) Deduceți că polinoamele

$$1, \frac{1}{1!}(X-a), \frac{1}{2!}(X-a)^2, \ldots, \frac{1}{n!}(X-a)^n$$

sînt liniar independente peste $\mathbf{R}$.

36.* Fie $p : \mathbf{R}^2 \to \mathbf{R}^2$, $p(x) = (0, x_2)$ oricare ar fi $x = (x_1, x_2) \in \mathbf{R}^2$. Arătați că p este o transformare liniară a lui $\mathbf{R}^2$ și $p \circ p = p$.

37.* Fie V un spațiu vectorial peste corpul K și $p \in \mathrm{End}_K(V)$ astfel încît $p \circ p = p$. Arătați că aplicația $q : V \to V$, $q(x) = x - p(x)$ oricare ar fi $x \in V$, este o transformare liniară a lui V și $q \circ q = q$.

38.* Fie V un spațiu liniar peste corpul K și $v_1, v_2, v_3 \in V$. Arătați că corespondența

$$f : K^3 \to V, \quad x = (\lambda_1, \lambda_2, \lambda_3) \mapsto f(x) = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3$$

este o aplicație liniară. Dacă (v_1, v_2, v_3) este o bază a lui V, atunci f este bijectivă. Generalizare.

39.* Pentru $\theta \in \mathbf{R}$ definim $f_\theta : \mathbf{R}^2 \to \mathbf{R}^2$ și $g_\theta : \mathbf{R}^2 \to \mathbf{R}^2$ prin

$$f_\theta(x) \overset{\text{def}}{=} (x_1 \cos\theta - x_2 \sin 0,\ x_1 \sin 0 + x_2 \cos\theta)$$

$$g_\theta(x) \overset{\text{def}}{=} (x_1 \cos\theta + x_2 \sin 0,\ x_1 \sin 0 - x_2 \cos\theta)$$

oricare ar fi $x = (x_1, x_2) \in \mathbf{R}^2$. Arătați că f_θ și g_θ sînt transformări liniare ale lui $\mathbf{R}^2$. Calculați $f_\theta \circ f_{\theta'}$, $g_\theta \circ g_{\theta'}$, $f_\theta \circ g_{\theta'}$, $g_\theta \circ f_{\theta'}$.

40.* Fie V un spațiu vectorial peste corpul $\mathbf{R}$ și $f \in \mathrm{End}_K(V)$ astfel încît $f \circ f = 1_V$,

$$V_1 = \{x + f(x) \mid x \in V\} \quad \text{și} \quad V_2 = \{x - f(x) \mid x \in V\}$$

1) Dacă $\alpha \in \mathbf{R}$, $u, v \in V_1(V_2)$, atunci αu, $u + v \in V_1$ (resp. V_2).

2) Pentru orice $x \in V$ există $y \in V_1$ și $z \in V_2$ unic determinați astfel încît $x = y + z$.

3) Dacă $V = \mathbf{R}^2$ și $f = g_\theta$ (v. Ex. 39) atunci $f \circ f = 1_V$. Cine sînt V_1 și V_2 cînd $\theta = \pi$?

41.* Dacă $x, y \in \mathbf{R}^2$, $x = (x_1, x_2)$, $y = (y_1, y_2)$ atunci notăm cu $\langle x, y\rangle$ numărul real $x_1y_1 + x_2y_2$. Arătați că:

1) $\langle x, x\rangle \geqslant 0$, $\forall x \in \mathbf{R}^2$ și $\langle x, x\rangle = 0 \Leftrightarrow x = 0$,

2) $\langle x, y\rangle = \langle y, x\rangle$, $\forall x, y \in \mathbf{R}^2$,

3) $\langle \alpha x + \alpha' x', y\rangle = \alpha\langle x, y\rangle + \alpha'\langle x', y\rangle$,

$\forall\ \alpha, \alpha' \in \mathbf{R}$ și $x, x', y \in \mathbf{R}^2$,

4) $\langle x, \beta y + \beta' y'\rangle = \beta\langle x, y\rangle + \beta'\langle x, y'\rangle$, $\forall \beta, \beta' \in \mathbf{R}$ și $x, y, y' \in \mathbf{R}^2$.

42.* Fie $A \in M_2(\mathbf{R})$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ și transformarea liniară $f_A : \mathbf{R}^2 \to \mathbf{R}^2$,

$$f_A(x) = (ax_1 + bx_2,\ cx_1 + dx_2),\ \forall x = (x_1, x_2) \in \mathbf{R}^2.$$

Următoarele afirmații sînt echivalente:

1) $\langle f_A(x), f_A(y)\rangle = \langle x, y\rangle$, $\forall x, y \in \mathbf{R}^2$

2) $\langle f_A(x), f_A(x)\rangle = \langle x, x\rangle$, $\forall x \in \mathbf{R}^2$,

3) Există $0 \in [0, 2\pi)$ astfel încît

$$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \quad \text{sau} \quad A = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

Dați o interpretare geometrică într-un plan euclidian a transformării liniare f_A care satisface proprietățile echivalente precedente.

INDICAȚII ȘI RĂSPUNSURI

CAPITOLUL I

3. 1) Pentru orice $x \in \mathbf{R}$ avem $(f_a, {}_b \circ f_c, {}_d)(x) = f_{a,b}\,(f_c, {}_d\,(x)) = acx + ad + b = f_{ac,\ ad+b}\,(x)$; 2) $\alpha = a^{-1}$, $\beta = a^{-1}b$.

4. Pentru orice $x \in \mathbf{Z} \times \mathbf{Z}$, $f_A(x)$ are a 2-a componentă pară, deci f_A nu este surjectivă; pentru orice $y \in \mathbf{Q} \times \mathbf{Q}$, $y = (y_1, y_2)$, sistemul de ecuații $3x_1 + x_2 = y_1$, $4x_1 + 2x_2 = y_2$ are soluție unică, deci f_A este bijectivă.

6. Primele egalități prin verificare directă. Apoi se poate continua astfel: $R_\theta S_{\theta'} = R_\theta R_{\theta'} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = R_{\theta+\theta'} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = S_{\theta+\theta'}$ etc.

7. Puneți condiția ca A să comute cu matricele $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ și se obține că 2) $\Rightarrow$ 1).

8. $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ și $A = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$.

12. Inducție după n (v. Teorema 4.2).

13. Avem $n^5 - n = (n-1)n(n+1) \cdot (n^2+1)$ și $240 = 2^4 \times 3 \times 5$ și se arată că $n^5 - n$ se divide prin 2^4, 3 și 5.

16. Se aplică regula lui Cramer.

17. Fie $e_1 = (1, 0)$, $e_2 = (0, 1)$. Cum $f_A(e_1) = f_B(e_1)$ rezultă că $(a_{11}, a_{21}) = (b_{11}, b_{21})$ iar din $f_A(e_2) = f_B(e_2)$ rezultă $(a_{12}, a_{22}) = (b_{12}, b_{22})$, deci $A = B$ etc.

18. Dacă $A^2 = -E$, atunci $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ cu $a, b, c \in \mathbf{Z}$, $a^2 + bc + 1 = 0$. De exemplu $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 3 & 5 \\ -2 & -3 \end{pmatrix}$.

19. Fie $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$. Atunci ${}^TA = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ și din ${}^TAA = E$ rezultă:

$$1 = \det(E) = \det({}^TA)\det(A) = (ad - bc)^2,$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E = {}^TAA = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a^2 + b^2 & ac + bd \\ ca + db & c^2 + d^2 \end{pmatrix},$$

deci $ad - bc = \pm 1$, $a^2 + b^2 = 1$, $ac + bd = 0$, $c^2 + d^2 = 1$. Dacă $ad - bc = 1$, atunci $c = -b$, $a = d$. Cum $a^2 + b^2 = 1$, există $0 \in [0, 2\pi)$ astfel încît $a = \cos\theta$ și $b = \sin\theta$ etc.

20. 4) $B = \frac{1}{2}(A + {}^TA)$, $C = \frac{1}{2}(A - {}^TA)$.

21. Există n astfel încît $a = bq_0 + r_0$, $b = r_0q_1 + r_1$, $r_0 = r_1q_2 + r_2$, ..., $r_{n-2} = r_{n-1}q_n + r_n$, $r_{n-1} = r_n q_{n+1} + 0$, cu $0 < r_n < r_{n-1} < \ldots < r_0 < b$ (algoritmul lui Euclid pentru a și b). Atunci:

$$r_n = (r_n, 0) = (r_{n-1}, r_n) = (r_{n-2}, r_{n-1}) = \ldots = (r_0, r_1) = (b, r_0) = (a, b).$$

22. Fie q, $r \in \mathbf{N}$ astfel încît $a = bq + r$, $0 \leqslant r < b$. Avem:

$$2^a - 1 = 2^{bq+r} - 1 = (2^{bq} - 1)2^r + 2^r - 1 = (2^b - 1)Q + 2^r - 1, \text{ unde}$$

$Q = (2^{b(q-1)} + 2^{b(q-2)} + \ldots + 2^b + 1)$ și $2^r - 1 < 2^b - 1$. Deci dacă r este restul împărțirii lui a prin b, atunci $2^r - 1$ este restul împărțirii lui $2^a - 1$ prin $2^b - 1$. În particular, dacă d este ultimul rest diferit de zero din algoritmul lui Euclid pentru a și b, atunci $2^d - 1$ este ultimul rest diferit de zero din algoritmul lui Euclid pentru $2^a - 1$ și $2^b - 1$, de unde $(2^a - 1, 2^b - 1) = 2^{(a,b)} - 1$.

23. Conform Ex. 22. este suficient să arătăm că numerele $6q - 1$, $6q + 1$, $6q + 2$, $6q + 3$, $6q + 5$, $6q + 7$ sînt relativ prime în perechi. Dacă un număr prim p divide două din ele, atunci divide și diferența lor în valoare absolută. Diferențele în valoare absolută posibile sînt 2, 3, 4, 6, 8, 1, 5, deci p poate fi 2, 3 sau 5. Se observă că 2 divide doar pe $6q + 2$ iar 3 doar pe $6q + 3$. Singura complicație poate apărea cînd 5 divide pe $6q + 2$ și $6q + 7$, ceea ce se exclude prin ipoteza $q \not\equiv 3 \pmod 5$.

24. Dacă $z = a + b\sqrt{2}$, $w = c + d\sqrt{2}$, atunci $zw = (ac + 2bd) + (ad + bc)\sqrt{2}$, de unde

$$f(zw) = \begin{pmatrix} ac + 2bd & 2(ad + bc) \\ ad + bc & ac + 2bd \end{pmatrix} = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}\begin{pmatrix} c & 2d \\ d & c \end{pmatrix} = f(z)f(w).$$

CAPITOLUL II

1. Vezi **Tablele II-1. și II-2.**

2. Vezi Tabla II-3.

3. Vezi Tablele II-4 și II-5.

4. Vezi Tablele II-6 și II-7.

5. Dacă $x, y \in (2, \infty)$ atunci $x - 2 > 0$, $y - 2 > 0$, deci $xy - 2(x + y) + 4 = (x - 2)(y - 2) > 0$. Cum $x * y = xy - 2(x + y) + 4 + \lambda - 4$, trebuie ca $\lambda \geqslant 6$.

6. Vezi Tabla II-8.

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Tabla II-1

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Tabla II-2

	0	1	2	3	4
0	0	1	2	3	4
1	1	0	1	2	3
2	2	1	0	1	2
3	3	2	1	0	1
4	4	3	2	1	0

Tabla II-3

$\perp$	α	β	γ
α	α	α	α
β	α	β	γ
γ	α	γ	γ

Tabla II-4.

$\top$	α	β	γ
α	α	β	γ
β	β	β	β
γ	γ	β	γ

Tabla II-5.

o	f_1	f_2	f_3
f_1	f_1	f_2	f_3
f_2	f_2	f_3	f_1
f_3	f_3	f_1	f_2

Tabla II-8.

$\perp$	1	2	3	4	6	12
1	1	1	1	1	1	1
2	1	2	1	2	2	2
3	1	1	3	1	3	3
4	1	2	1	4	2	4
6	1	2	3	2	6	6
12	1	2	3	4	6	12

Tabla II-6

$\top$	1	2	3	4	6	12
1	1	2	3	4	6	12
2	2	2	6	4	6	12
3	3	6	3	12	6	12
4	4	4	12	4	12	12
6	6	6	6	12	6	12
12	12	12	12	12	12	12

Tabla II-7.

7. Elementul neutru este 0. Dacă $x, y \in [-1, \infty)$ atunci $x + 1 \geqslant 0$, $y + 1 \geqslant 0$, deci $x + y + xy + 1 = (y + 1)(x + 1) \geqslant 0$, de unde $x * y \in [-1, \infty)$.

8. Operația „$\perp$" admite ca element neutru pe b cînd H este $[a, b]$ sau $(a, b]$ iar operația „$\top$" admite ca element neutru pe a cînd H este $[a, b]$ sau $[a, b)$.

9. Operația „$\top$" admite ca element neutru pe 1. Operația „$\perp$" nu admite element neutru, iar cea indusă pe H de „$\perp$" admite ca element neutru pe 12.

12. Dacă $e \in \mathbf{Z}$ este element neutru, puneți condițiile $e * 0 = 0$ și $e * 1 = 1$.

13. $(1, n, p)$, $(m, n, 1)$ $(m, 2; 2)$;

14. $a = 0$, $b = 0$, sau $a = \frac{1}{2}$, $b = 1$.

15. $e = 2$.

16. 3) Avem $AV = A$, $\forall A \in M$ dacă $V = \begin{pmatrix} 0 & c \\ 0 & 1 \end{pmatrix}$ cu $c \in \mathbf{R}$.

18. Operația „$*$" nu este asociativă și admite element neutru matricea $\frac{1}{2}E$, unde E este matricea unitate.

20. Fie $x, y \in H$, $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$, Atunci $xy = (ac + 2bd) + (ad + bc)\sqrt{2}$ și $(ac + 2bd)^2 - 2(ad + bc)^2 = a^2(c^2 - 2d^2) - 2b^2(c^2 - 2d^2) = 1$, deci $xy \in H$. Cum $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 = 1$, avem $x^{-1} = a - b\sqrt{2}$.

21. 2) A este simetrizabil dacă și numai dacă $a \neq 0$ și $b \neq 0$ și avem $A^{-1} = \begin{pmatrix} a^{-1} & 0 \\ -ca^{-1}b^{-1} & b^{-1} \end{pmatrix}$.

24. $x = 1$, $y = 2$.

25. Elementul neutru este $(1, 0)$, elementele simetrizabile sînt $(1, b)$ și $(-1, b)$ cu $b \in \mathbf{Z}$.

26. Fie $b \in M$ astfel încît $a = aba$. Fie $e = ab$ și $f = ba$. Avem $ey = abaxa = axa = y$ și $yf = axaba = axa = y$, $\forall y \in M$. În particular $e = ef = f$.

27. Luînd x arbitrar, $y = e$, $u = e$ și $v = e'$ se obține $x = x \perp e$. Luînd $x = e'$, $y = e$, $u = e$ și v arbitrar se obține $v = e \perp v$, de unde $e = e'$. Acum avem $x \perp y = (x \top e) \perp (e \top y) = (x \perp e) \top (e \perp y) = x \top y$, $\forall x, y \in M$. De asemenea, $x \perp y = (e \top x) \perp (y \perp e) = (e \perp y) \top (x \perp e) = y \top x = y \perp x$.

28. 1) 3^9; 2) 3^6; 3). 3^5. În general, pentru o mulțime cu n elemente, avem: n^{n^2}, $n^{n(n+1)/2}$, $n^{(n-1)^2+1}$ respectiv.

30. Orice cuvînt $\alpha \in M$ se poate scrie sub forma $\alpha = \alpha'\alpha''$, unde α' este secvența formată cu primele 5 litere ale lui α și α'' este secvența formată cu următoarele 3 litere ale lui α. Dacă $\alpha, \beta, \gamma \in M$, $\alpha = \alpha'\alpha''$, $\beta = \beta'\beta''$, $\gamma = \gamma'\gamma''$, atunci $(\alpha * \beta) * \gamma = (\alpha'\beta'') * (\gamma'\gamma'') = \alpha'\gamma'' = (\alpha'\alpha'') * (\beta'\gamma'') = \alpha * (\beta * \gamma)$.

CAPITOLUL III

1. ± 1, $\pm i$.

2. Dacă $x, y \in (-1, 1)$, atunci $(x + y)/(x + xy) \in (-1, 1)$.

Elementul neutru este 0 iar simetricul lui x este $-x$.

3. Vezi Tabla III-1. **4.** Vezi Tabla III-2. **5.** Vezi Tabla III-3.

$\cdot$	1	ε	ε^2
1	1	ε	ε^2
ε	ε	ε^2	1
ε^2	ε^2	1	ε

Tabla III-1.

o	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

Tabla III-2.

o	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_3	f_1	f_6	f_4	f_5
f_3	f_3	f_1	f_2	f_5	f_6	f_4
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

Tabla III-3.

10. Avem $xyxy = xxyy$. Înmulțind la stînga cu x^{-1} și la dreapta cu y^{-1}, rezultă $xy = yx$.

11. Avem $(xy)^2 = e = ee = x^2y^2$ și se aplică Ex. 10.

12. Pentru x arbitrar și $y = e$ rezultă $x = (x \top x) \top x$. Deci $x \top x = e$, de unde $x \perp y = x \top y$. Aplicînd Ex. 11 deducem și $x \perp y = y \perp x$.

13. $\xi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. **14.** $x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$, $y = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$

15. Cînd $h \geqslant 0$ și $k \geqslant 0$ vezi Ex. R-2, § 9, Cap. II. Dacă $h < 0$ și $k < 0$, atunci $a^hb^k = (a^{-h})^{-1}(b^{-k})^{-1} = (b^{-k}a^{-h})^{-1} = (a^{-h}b^{-k})^{-1} = (b^{-k})^{-1}(a^{-h})^{-1} = b^ka^h$ etc.

16. Din $ab = b^4a$ rezultă că $b^4 = aba^{-1}$. Atunci $b^2 = b^2b^6 = b^4b^4 = aba^{-1}aba^{-1} = ab^2a^{-1}$, de unde $b^2a = ab^2$. Atunci $ab^3 = b^2ab = b^2b^4a = a$, de unde $b^3 = e$. Înmulțind la stînga și dreapta cu b egalitatea $b^2a = ab^2$ rezultă $ab = ba$.

17. Vezi Teoremele 4.1 și 4.2, Cap. IV, § 4.

19. Evident $12\mathbf{Z} \subseteq 3\mathbf{Z} \cap 4\mathbf{Z}$. Dacă $a \in 3\mathbf{Z} \cap 4\mathbf{Z}$, atunci $3 \mid a$ și $4 \mid a$ și cum $(3, 4) = 1$ rezultă că $3 \times 4 = 12$ divide a, deci $a \in 12\mathbf{Z}$.

21. a) $H = (\mathbf{Z}, +)$; b) $H = (\mathbf{Q}, +)$.

25. Se observă că $f(x) \in (-1, 1)$, $\forall x \in (0, \infty)$ și $f(xy) = f(x) * f(y)$.

26. Funcția $f : G \to \mathbf{R}$, $f(x) = \operatorname{tg}(x)$, $\forall x \in G$ este un izomorfism de la $(G, *)$ la $(\mathbf{R}, +)$.

27. 1) Vezi Tabla III-4. 2) Definiți $f : \mathcal{K} \to G$ prin $f(e) = E$, $f(u) = A$, $f(v) = B$ și $f(w) = E$.

$\cdot$	E	A	B	C
E	E	A	B	C
A	A	E	C	B
B	B	C	E	A
C	C	B	A	E

Tabla III-4

Δ	$\varnothing$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\varnothing$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\{a\}$	$\{a\}$	$\varnothing$	$\{a, b\}$	$\{b\}$
$\{b\}$	$\{b\}$	$\{a, b\}$	$\varnothing$	$\{a\}$
$\{a, b\}$	$\{a, b\}$	$\{b\}$	$\{a\}$	$\varnothing$

Tabla III-5.

29. 1) Vezi Tabla III-5; 2) $f(e) = \varnothing$, $f(u) = \{a\}$, $f(v) = \{b\}$, $f(w) = \{a, b\}$.

32. 2) Punînd condiția $f(xy) = f(x) * f(y)$ rezultă că $(ab - 3a)x + (ab - 3a)y + b^2 - 7b + 12 = 0$, $\forall x, y \in \mathbf{R}$. Deducem că $a = 1$ și $b = 3$.

33. Fie $G = \{e, a, b, c\}$. Dacă $x^2 = e$, $\forall x \in G$, atunci $G \simeq \mathcal{K}$ (v. Ex. R-1, § 6). Altfel, există $x \in G$ astfel încît $x^2 \neq e$. În acest caz $G = \{e, x, x^2, x^3\}$ și $x^4 = e$, de unde $G \simeq \mathcal{R}_4$.

34. Numărul elementelor mulțimii $G \setminus \{e\}$ este impar. Dacă $a^{-1} \neq a$ oricare ar fi $a \neq e$, atunci $G \setminus \{e\}$ poate fi scrisă ca reuniune disjunctă de submulțimi cu cîte două elemente de forma $\{a, a^{-1}\}$, cu $a \neq e$. Contradicție.

35. Avem $x^k y^k xy = (xy)^k xy = (xy)^{k+1} = x^{k+1} y^{k+1}$. Înmulțind egalitatea $x^k y^k xy = x^{k+1} y^{k+1}$ la stînga cu x^{-k} și la dreapta cu y^{-1} se obține $y^k x = xy^k$. Analog avem $y^{k-1} x = xy^{k-1}$. Din $y^k x = xy^k$ și $y^{k-1} x = xy^{k-1}$ se obține $xy = yx$.

36. 1) $\Rightarrow$ 2) Fie $a \in H$. Cum H este mulțime finită, aplicația $f : H \to H$, $f(x) = ax$, este bijectivă. Există deci $b \in H$ astfel încît $ab = a$. Atunci $b = e$, deci $e \in H$. Există $a' \in H$ astfel încît $aa' = e$. Dar $a^{-1} = a' \in H$ și deci H este subgrup.

37. 2) $\Rightarrow$ 1) Există $e \in G$ astfel încît $ae = a$. Pentru $b \in G$ avem $be = yae = ya = b$. Analog există $e' \in G$ astfel încît $e'b = b$, $\forall b \in G$. Evident, $e = e'$. Dacă $a \in G$, există a', $a'' \in G$ astfel încît $a'a = e = aa''$ și cum $a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$ se deduce că a^{-1} există.

40. 1) $\Rightarrow$ 2). Dacă $H = 0 = \{0\}$ se ia $n = 0$. Dacă $H \neq 0$ fie $x \in H$, $x \neq 0$. Cum și $-x \in H$ rezultă că H conține numere întregi strict pozitive și fie $n > 0$ cel mai mic număr strict pozitiv din H. Avem $n\mathbf{Z} \subseteq H$ și folosind teorema împărțirii (prin n) cu rest se arată și $H \subseteq n\mathbf{Z}$.

42. Dacă H este finit există $h, k \in \mathbf{Z}$, $h \neq k$, astfel încît $z^h = z^k$, deci $z^{h-k} = 1$. Atunci $z = \cos\varphi + i \sin\varphi$, deci $\cos(h - k)\varphi + i \sin(h - k)\varphi = 1$, de unde $(h - k)\varphi = 2\pi t$, $t \in \mathbf{Z}$. Rezultă că $\varphi = 2\pi\alpha$, unde $\alpha = t/(h - k) \in \mathbf{Q}$.

44. Fie $\zeta_n = \cos\frac{2\pi}{p^n} + i \sin\frac{2\pi}{p^n}$. Din Ex. R-2, § 5 rezultă că $U_{p^n} = \{1, \zeta_n, \ldots, \zeta_n^{p^n-1}\}$. Dacă $\zeta_n \in H$, $\forall n \geqslant 0$, atunci $U_{p^n} \leqslant H$, $\forall n \geqslant 0$, de unde $H = C_{p^\infty}$. Contradicție. Există n astfel încît $\zeta_n \in H$ și $\zeta_{n+1} \notin H$. Arătați că $H = U_{p^n}$.

CAPITOLUL IV

1. Elementul zero al lui A este $(0, 0)$, elementul unitate este $(1, 0)$. Dacă $(a, b)(x, y) = (0, 0)$, atunci $ax + 3by = 0$ și $bx + ay = 0$. Cînd $(a, b) \neq (0, 0)$ avem $\det\begin{pmatrix} a & 3b \\ b & a \end{pmatrix} = a^2 - 3b^2 \neq 0$, de unde $x = 0$, $y = 0$, deci A nu are divizori ai lui zero.

3. Dacă „$\perp$" și „$\top$" satisfac condițiile din enunț, atunci pentru orice $x, y \in \mathbf{Z}$ avem $x + y - a = (x - a) \perp (y - a)$ și $xy - a = (x - a) \top (y - a)$. Observînd că f este bijectiv și notînd $x - a = u$, $y - a = v$, avem $u \perp v = u + v + a$ și $u \top v = uv + au + av - a^2 - a$, $\forall u, v \in \mathbf{Z}$. Elementul zero este $-a$, elementul unitate este $1 - a$.

5. Elementul zero este $(0, 0)$ iar $(1, 0)$ este elementul unitate al lui A. Elementele inversabile sînt $(1, 0)$, $(-1, 0)$, $(0, 1)$ și $(0, -1)$.

7. 1) $(1, 1)$, $(1, -1)$, $(2, 1)$, $(2, -1)$, $(4, 1)$, $(4, -1)$, $(5, 1)$, $(5, -1)$, $(7, 1)$, $(7, -1)$, $(8, 1)$, $(8, -1)$.

8. Vezi Tablele IV.1 și IV.2.

$+$	$(0, 0)$	$(1, 0)$	$(0, 1)$	$(1, 1)$
$(0, 0)$	$(0, 0)$	$(1, 0)$	$(0, 1)$	$(1, 1)$
$(1, 0)$	$(1, 0)$	$(0, 0)$	$(1, 1)$	$(0, 1)$
$(0, 1)$	$(0, 1)$	$(1, 1)$	$(0, 0)$	$(1, 0)$
$(1, 1)$	$(1, 1)$	$(0, 1)$	$(1, 0)$	$(0, 0)$

Tabla IV.1

$\cdot$	$(0, 0)$	$(1, 0)$	$(0, 1)$	$(1, 1)$
$(0, 0)$	$(0, 0)$	$(0, 0)$	$(0, 0)$	$(0, 0)$
$(1, 0)$	$(0, 0)$	$(1, 0)$	$(0, 0)$	$(1, 0)$
$(0, 1)$	$(0, 0)$	$(0, 0)$	$(0, 1)$	$(0, 1)$
$(1, 1)$	$(0, 0)$	$(1, 0)$	$(0, 1)$	$(1, 1)$

Tabla IV.2

9. $x + x = (x + x)^2 = (x + x)(x + x) = x^2 + x^2 + x^2 + x^2 = x + x + x + x$, de unde $x + x = 0$ și deci $x = -x$, $\forall x \in B$. De asemenea, $x + y = (x + y)^2 = (x + y)(x + y) = x^2 + yx + xy + y^2 = x + yx + xy + y$, de unde $yx + xy = 0$, deci $yx = -xy = xy$.

10. 1) 16; 3) Există 6 elemente inversabile.

14. 1) $a \oplus a \oplus a \oplus a \oplus a = (1 \oplus 1 \oplus 1 \oplus 1 \oplus 1) * a = 0 * a = 0$.

2) Se observă că $5 \mid C_5^k$, $0 < k < 5$ și se aplică 1) și Ex. 13.

15. 1) Oricare ar fi $a, b, c \in \mathbf{R}$ cu $ac = 0$; 2) $(E - U)(E + U) = E$.

16. Vezi Tabla IV.3.

17. $x = \hat{2}$, $y = \hat{1}$.

22. Vezi Tablele IV.4 și IV.5.

·	$\hat{1}$	$\hat{5}$	$\hat{7}$	$\hat{11}$
$\hat{1}$	$\hat{1}$	$\hat{5}$	$\hat{7}$	$\hat{11}$
$\hat{5}$	$\hat{5}$	$\hat{1}$	$\hat{11}$	$\hat{7}$
$\hat{7}$	$\hat{7}$	$\hat{11}$	$\hat{1}$	$\hat{5}$
$\hat{11}$	$\hat{11}$	$\hat{5}$	$\hat{7}$	$\hat{1}$

Tabla IV.3

+	0	E	U	V
0	0	E	U	V
E	E	0	V	U
U	U	V	0	E
V	V	U	E	0

Tabla IV.4

·	0	E	U	V
0	0	0	0	0
E	0	E	U	V
U	0	U	V	E
V	0	V	E	U

Tabla IV.5

24. 2) (1, 0), (−1, 0), (0, 1), (0, −1); 2) Aplicația $f : \mathbf{Z}[i] \to A$, $f(z) = (a, b)$, $\forall z \in \mathbf{Z}[i]$, $z = a + ib$, este izomorfism.

26. Aplicația $f : \mathbf{C} \to K$, $f(z) = (a, b)$, $\forall z \in \mathbf{C}$, $z = a + ib$ este izomorfism.

27. Aplicația $f : K \to \mathbf{R}$, $f(x) = \ln x$, $\forall x \in K$, este un izomorfism.

28. Aplicația $f : I \to K$, $f(0) = (\hat{0}, \hat{0})$, $f(E) = (\hat{0}, \hat{1})$, $f(U) = (\hat{1}, \hat{0})$, $f(V) = (\hat{1}, \hat{1})$ este izomorfism.

29. Aplicația $f : \mathbf{Q}(\sqrt{2}) \to K$, $f(z) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$, $\forall z \in \mathbf{Q}(\sqrt{2})$, $z = a + b\sqrt{2}$ este izomorfism.

30. 1) $a = b = i$, $i = 6$; 2) $\alpha = a$, $\beta = 2$.

31. Dacă $a, b \in Z(A)$ atunci $(a + b)x = ax + bx = xa + xb = x(a + b)$, $(ab)x = a(bx) = a(xb) = (xa)b = x(ab)$ și $(-a)x = -(ax) = -(xa) = (-x)a$, $\forall x \in A$, deci $a + b$, ab, $-a \in Z(A)$. Cum $xy + yx = (x + y)^2 - (x + y) + x - x^2 + y - y^2 \in Z(A)$, avem $x(xy + yx) = (xy + yx)x$, deci $x^2y = yx^2$, de unde $x^2 \in Z(A)$, $\forall x \in A$. În fine, pentru orice $x \in A$ avem $x = (x - x^2) + x^2 \in Z(A)$, de unde $xy = yx$, $\forall x, y \in Z(A)$. Cînd $A = M_2(\mathbf{R})$ avem $U \in Z(A) \Leftrightarrow U = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, $a \in \mathbf{R}$.

33. 1) Conform cu Ex. R-2, § 2 grupul $(U(\mathbf{Z}_n), \cdot)$ are $\varphi(n)$ elemente și aplicînd Ex. R-4, § 4, Cap. III rezultă că $\hat{a}^{\varphi(n)} = \hat{1}$, $\forall a \in \mathbf{Z}$, $(a, n) = 1$. Deci $\widehat{a^{\varphi(n)}} = \hat{1}$, de unde $a^{\varphi(n)} \equiv 1 \pmod{n}$.

34. 2) Se aplică Ex. R-4, Cap. I și pct. 1); 3) $\varphi(p^2q^3) = p(p - 1)q^2(q - 1)$.

35. Cum $(3, 5) = 1$ rezultă că $3^{\varphi(5)} = 1 \pmod 5$ deci $5 \mid (3^4 - 1)$ și avem $3^4 - 1 = 5 \times 16$. Avem $3 \cdot 3^3 + 5(-16) = 1$ și atunci $x_0 = 3^3 \times 2 = 54$, $y_0 = (-16) \times 2 = -32$ este o soluție particulară a ecuației $3x + 5y = 2$. Din $3x_0 + 5y_0 = 2$ și $3x + 5y = 2$ rezultă $3(x - x_0) = 5(y_0 - y)$. Deducem că $3 \mid (y_0 - y)$ și $5 \mid (x - x_0)$. Mai mult $x = x_0 + 5t$ și $y = y_0 - 3t$ cu $t \in \mathbf{Z}$.

40. Se observă că $f(r) = r$, $\forall r \in \mathbf{Q}$ (v. Ex. R-3, § 5). Dacă $x \in \mathbf{R}$, $x > 0$, atunci $f(x) \triangleright 0$. În adevăr, fie $y \in \mathbf{R}$, $y > 0$ astfel încît $y^2 = x$. Atunci $f(x) = f(y^2) = (f(y))^2 = (f(y))^2 \triangleright 0$.

Fie $x \in \mathbf{R}$, $\varepsilon > 0$ și $r_1, r_2 \in \mathbf{Q}$, $x - \varepsilon < r_1 < x < r_2 < x + \varepsilon$. Atunci $f(x - \varepsilon) \triangleleft f(r_1) < f(x) < f(r_2) < f(x + \varepsilon)$, deci $r_1 < f(x) < r_2$, de unde $|f(x) - x| < \varepsilon$. Rezultă că $f(x) = x$, $\forall x \in \mathbf{R}$.

CAPITOLUL V

1. $f + g = X^2 + \hat{4}X + \hat{4}$, $fg = X^6 + X^5 + \hat{4}X^4 + \hat{4}X^3 + \hat{2}X + \hat{3}$.

2. $fg = 0$.

3. $\hat{2}X^3 + \hat{2}X^2 + \hat{1}$, $X^3 + \hat{2}X^2 + X + \hat{1}$, $\hat{2}X^3 + \hat{2}X + \hat{1}$.

4. $\hat{0}$, $\hat{1}$, $\hat{2}$, $\hat{3}$, $\hat{4}$, $\hat{5}$.

5. Fie $f = ax + b$, $g = cX + d$. Punînd condiția $f^2 + g^2 = X^2 + 1$ rezultă $a^2 + c^2 = 1$, $b^2 + d^2 = 1$, $ab + cd = 0$. De asemenea, $(2a + b)^2 + (2c + d) = 5$, $(2a + b)(2c + d) = 2$. Deci $2a + b$ și $2c + d$ sînt rădăcinile ecuației $t^2 - 5t + 2 = 0$. Se găsește $f = \frac{4}{5}X + \frac{3}{5}$, $g = \frac{3}{5}X - \frac{4}{5}$ etc.

6. grad f este 0 dacă $\lambda = 1$, 2 dacă $\lambda = 2$, 3 dacă $\lambda \neq 2$ și $\lambda \neq 1$.

7. $f = X + 2$, $g = -X - 1$.

10. $q = 2X^2 + X - i$, $r = -iX$.

11. $q = \hat{4}X^2 + \hat{4}X + \hat{2}$, $r = \hat{3}X + \hat{2}$.

12. $a = 14$, $b = -3$.

13. $f = -1 + 4X - 6X^2 + 4X^3$.

14. $a = \pm i$, $b = 0$; $a = 1$, $b = \pm\sqrt{2}$; $a = -1$, $b = \pm i\sqrt{2}$.

16. $f = X^3 - 6X^2 + 15X - 15$.

17. $f(3) = 196$.

18. $q = \hat{5}X^3 + \hat{3}X^2 + \hat{2}X + \hat{5}$, $r = \hat{5}$.

19. $f(-2 - i) = -1 - 44i$.

20. $f = (X + 1)^4 - 2(X + 1)^3 - 3(X + 1)^2 + 4(X + 1) + 1$, $g = (X + 1)^3 - 2i(X + i)^3 - (1 + i)(X + i)^2 - 5(X + i) + 7 + 5i$.

21. $a = 0$, $b = 0$, $c = -1$, $d = 1$.

22. $f = 3X^5 - 10X^3 + 15X$.

23. $n = 2$, $n = 3$.

24. $F(x) = \dfrac{1}{(x-2)^2} + \dfrac{6}{(x-2)^3} + \dfrac{11}{(x-2)^4} + \dfrac{7}{(x-2)^5}$;

$$G(x) = \frac{1}{x+1} - \frac{4}{(x+1)^2} + \frac{4}{(x+1)^3} + \frac{2}{(x+1)^5}.$$

25. $f = (X-1)^2\,(X^{n-1} + 2X^{n-2} + 3X^{n-3} + \ldots + (n-1)X + n)$.

26. Fie $a, b \in \mathbf{Z}$, $a = 2s$, $b = 2t+1$ astfel încît $f(a) = f(b) = 0$. Cum $a \neq b$, polinomul $(X-a)\,(X-b)$ divide pe f, deci există $q \in \mathbf{Z}[X]$ astfel încît $f = (X-2s)\,(X-2t-1)q$. Se observă că pentru orice $k \in \mathbf{Z}$ unul din numerele $k-2s$, $k-2t-1$ este par.

27. a) $X^2 + X + 1$; b) 1; c) $X - 1$; d) $\hat{1}$; e) $X^2 + \hat{3}$.

28. $a = 6$, $b = 7$.

29. $\lambda = 2$, $\mu = -1$, $(f, g) = X^2 - 4X + 3$.

30. $X^4 + 4 = (X^2 + 2X + 2)\,(X^2 - 2X + 2) = (X + 1 - \mathrm{i})\,(X + 1 + \mathrm{i})\,(X - 1 + \mathrm{i})\,(X - 1 - \mathrm{i})$, $X^6 + 27 = (X^2 + 3)\,(X^2 + 3X + 3)\,(X^2 - 3X + 3) = (X + \mathrm{i}\sqrt{3})\,(X - \mathrm{i}\sqrt{3})\,(X + z)\,(X + \bar{z})\,(X - z)\,(X - \bar{z})$, unde $z = (3 + \mathrm{i}\sqrt{3})/2$.

31. $f = (X + \hat{2})\,(X + \hat{3})\,(X^2 + X + \hat{1})$.

32. 1) v. Exp. 2, § 6; 2) $f = (X - \sqrt[3]{2})\,(X^2 + \sqrt[3]{2}\,X + \sqrt[3]{4}) = (X - \sqrt[3]{2})\,(X - \sqrt[3]{2}\,\varepsilon)\,(X - \sqrt[3]{2}\,\varepsilon^2)$, unde $\varepsilon = (-1 + \mathrm{i}\sqrt{3})/2$.

33. a) $e = 3$, $f = (X-2)^3\,(X^2 + X + 1)$; b) $e = 4$, $f = (X+2)^4\,(X-1)$.

34. $\lambda = -5$.

35. $a = 4$, $b = -5$.

38. 1 este rădăcină independentă de a și este dublă cînd $a = (1 \pm \sqrt{21})/2$, iar $-1/2$ este rădăcină dublă cînd $a = (-5 \pm \sqrt{57}))/6$.

41. Pentru $a = 1\,(-1,\ 5\sqrt{3}/9,\ -5\sqrt{3}/9)$ rădăcina dublă este 1 (resp. $-1, \sqrt{3}/3, -\sqrt{3}/3$).

42. a) $1, -4, 2/3$; b) $a, 3a, -4a$; c) $2 + \sqrt{10}, 2 - \sqrt{10}, 2\mathrm{i}, 3\mathrm{i}$; d) $3, 4, 5$ și $a = 47$.

43. $\pm 1, \pm 2, 5$.

45. -50.

46. $X^3 + 2aX^2 + a^2X - b^2$.

47. $a = 2$.

48. $a = -2;\ \dfrac{1}{2},\ 1,\ 2$.

49. $a = -6$, $b = -9$.

51. a) $a = -3$, $b = 2$ și rădăcinile $2 \pm \sqrt{2}$, $(-1 \pm \mathrm{i}\sqrt{3})/2$; b) $a = -1$, $b = -2$ și rădăcinile $(3 \pm \sqrt{5})/2$, $(-1 \pm \mathrm{i}\sqrt{3})/2$.

55. Rădăcinile polinomului g sînt $\varepsilon = (-1 + \mathrm{i}\sqrt{3})\,2$ și ε^2. Cum $\varepsilon^3 = \bar{\varepsilon}^3 = 1$, rezultă că $f(\varepsilon) = f(\bar{\varepsilon}) = 0$, deci f se divide prin $(X - \varepsilon)\,(X - \bar{\varepsilon}) = X^2 + X + 1$.

56. $a = -10$, $b = 18$, $1 \pm \mathrm{i}$, $-2 \pm \mathrm{i}\sqrt{5}$.

58. $-1/2;\ 1, 1, -3, -3;\ 1/2$.

59. $1/6$.

60. Dacă $f = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$, deduceți că a_0 este impar și că numărul coeficienților impari printre $a_n, a_{n-1}, \ldots, a_1$ este par.

61. Restul împărțirii lui $(a + bX)\,(c + dX)$ prin $X^2 + 1$ este $(ac - bd) + (ad + bc)X$, deci $(a + bX) * (c + dX) = (ac - bd) + (ad + bc)X$. Aplicația $f : \mathbf{C} \to K$, $f(z) = a + bX$, $\forall z \in \mathbf{C}$, $z = a + b\mathrm{i}$, este un izomorfism.

62. Vezi Ex. 61.

68. $f = a(X-1)\,(X-2)\,(X-3)$.

69. $n = 3$.

71. Din primele două relații între rădăcini și coeficienți se deduce $(x_1 - 1)^2 + (x_2 - 1)^2 + (x_3 - 1)^2 + (x_4 - 1)^2 = 0$ și cum rădăcinile sînt reale, rezultă $x_1 = x_2 = x_3 = x_4 = 1$.

72. Orice polinom $f \in \mathbf{Q}[X]$, $f \neq 0$, care admite pe $\sqrt[3]{2}$ ca rădăcină se divide prin polinomul $g \neq 0$, $g \in \mathbf{Q}[X]$ de grad minim care admite pe $\sqrt[3]{2}$ ca rădăcină. Aplicați acum Ex. 65.

73. $-1, -2, -3, \ldots, -n$.

74. $S = -2^n(n+2)/(2^{n+1} - 1)$.

75. Fie $f = a_nX^n + \ldots + a_1X + a_0$ și $r = p/q$ o rădăcină rațională, unde p/q este fracție ireductibilă. Avem $a_np^n + a_{n-1}q + \ldots + a_1pq^{n-1} + a_0q^n = 0$. Arătați imposibilitatea ultimei egalități, oricare ar fi paritatea posibilă a lui p și q.

77. Vezi demonstrația Teoremei 4.2. Cap. I.

78. Inducție după n.

79. Vezi Ex. R-3, § 4.

80. Este suficient să arătăm că nu există g, $h \in \mathbf{Z}[X]$, $g = b_0 + bX + \ldots + b_qX^q$, $h = c_0 + c_1X + \ldots + c_rX^r$ cu $b_q \not\equiv 0$, $c_r \not\equiv 0$, $q < n$ și $r < n$, astfel încît $f = gh$. Presupunem contrariul. Cum $a_0 = b_0c_0$, $a_0 \equiv 0 \pmod p$ și $a_0 \not\equiv 0 \pmod{p^2}$ avem de exemplu $b_0 \equiv 0 \pmod p$ și $c_0 \not\equiv 0 \pmod p$. Cum $a_n = b_qc_r$ și $a_n \not\equiv 0 \pmod p$, avem $b_q \not\equiv 0 \pmod p$. Fie k minim astfel încît $b_k \not\equiv 0 \pmod p$. Cum $a_k = b_kc_0 + \sum_{i=0}^{k-1} b_ic_{k-i}$ și $k \leqslant q < n$ avem $p \mid a_k$, de unde $p \mid b_kc_0$. Contradicție.

CAPITOLUL VI

3. Avem $f * (g * x) = f * (g(x)) = f(g(x)) = (f \circ g)(x) = (f \circ g) * x$; $1_M * x = 1_M(x) = x$.

6. K^n are 2^n vectori.

7. K^n, unde $K = \mathbf{Z}_p$.

8. Fie $v \in V$, $v \neq 0$. Atunci aplicația $\mathbf{R} \to V$, $\alpha \to \alpha v$ este injectivă.

9. $x + x + \ldots + x = \hat{1}x + \hat{1}x + \ldots + \hat{1}x = (\hat{1} + \hat{1} + \ldots + \hat{1})x = \hat{p}x = \hat{0}x = 0$.

11. $v = (-3)v_1 + 0 \cdot v_2 + 5v_3$.

12. $A = -5E_1 - E_2 + 6E_3 - 2E_4$.

13. $f = 3f_1 - 9f_2 + 5f_3$.

14. $f = 1 + (-1)X + (-1)X^2 + X^3 = 1 \cdot (1 + X^2) + (-1)(X + X^2) + (-2)X^2 + 1 \cdot (X^3 + X^2) = 0$. $1 + 0(X-1)/1! + 4(X-1)^2/2! + 6(X-1)^3/3!$.

17. $v = 2v_1 - v_2 + 3v_3$; $w = v_1 - 2v_2 + 2v_3$.

18. $v = 2v_1 - 3v_2 - 2v_3 + 3v_4$.

19. $v = \hat{4}v_1 + \hat{1} \cdot v_2 + \hat{3} \cdot v_3$.

20. 1) $x_1 = 5$, $x_2 = 6$, $x_3 = 10$; 2) $x_1 = 0$, $x_2 = -1$, $x_3 = -1$, $x_4 = 2$.

21. $A^{-1} = \begin{pmatrix} 1/12 & 1/4 & -5/12 \\ 1/3 & 0 & 1/3 \\ -1/4 & 1/4 & 1/4 \end{pmatrix}$, $B^{-1} = \begin{pmatrix} 2 & 3 & -4 \\ 1 & 1 & -1 \\ 4 & 5 & -1 \end{pmatrix}$,

$$C^{-1} = \begin{pmatrix} 0 & 1 & -1 \\ 2/3 & 0 & -1/3 \\ -1/3 & -1 & 5/3 \end{pmatrix}$$

22. $A^{-1} = \begin{bmatrix} \hat{2} & \hat{2} & \hat{2} \\ \hat{2} & \hat{0} & \hat{1} \\ \hat{0} & \hat{2} & \hat{2} \end{bmatrix}$, $B^{-1} = \begin{bmatrix} \hat{2} & \hat{1} & \hat{2} \\ \hat{2} & \hat{2} & \hat{1} \\ \hat{1} & \hat{2} & \hat{2} \end{bmatrix}$.

23. v_1, v_2, v_4.

24. v_1, v_3.

25. 1) $f = (\hat{X} - \hat{3})^3 + 6(X-3)^2 + 5(X-3) - 2$; 2) $f = (X - \hat{2})^3 + \hat{3}(X - \hat{2})^2 + \hat{4}(X - \hat{2}) + \hat{2}$.

26. $f^3 = 1_{\mathbf{R}}$.

27. 2) $\lambda_1 = 3$, $\lambda_2 = -2$; Fie $\alpha, \beta \in \mathbf{R}$ astfel încît $\alpha x + \beta y = 0$. Aplicînd f obținem $\alpha\lambda x + \beta\mu y = 0$, de unde $\beta(\mu - \lambda)y = 0$, deci $\beta = 0$ și apoi obținem și $\alpha = 0$.

28. Folosiți faptul că $X^3 - 2$ este polinomul $\neq 0$ de grad minim cu coeficienți din $\mathbf{Q}$ care admite pe $\sqrt[3]{2}$ ca rădăcină.

29. Aplicați regula lui Cramer.

30. Dacă $v_i = \alpha_1v_1 + \ldots + \alpha_{i-1}v_{i-1} + \alpha_{i+1}v_{i+1} + \ldots + \alpha_mv_m$, atunci $v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_m$ este, de asemenea, sistem de generatori. Aplicați apoi Teorema 4.1.

31. 1) Inducție după r. Cînd $r = 1$ afirmația rezultă din lema substituției. Presupunem că afirmația este adevărată pentru $r - 1$ și apoi printr-o nouă aplicare a lemei substituției rezultă și pentru r; 2) Rezultă din 1).

32. Se aplică Teorema 4.1 și teorema bazei (v. Ex. 31).

33. 3) $\Rightarrow$ 1) Se aplică Ex. 30 și teorema bazei.

34. Avem $-(y + x) = (-x) + (-y) = (-1)x + (-1)y = (-1)(x + y) = -(x + y)$, de unde $x + y = -(-(x + y)) = -(-(y + x)) = y + x$.

35. Fie $m_i = \operatorname{grad} f_i$, $f_i = a_iX^{m_i} + \ldots +$, $a_i \neq 0$, $1 \leqslant i \leqslant n$. Putem presupune că $m_1 < m_2 < \ldots < m_n$. Dacă $\alpha_1f_1 + \ldots + \alpha_nf_n = 0$ și nu toți scalarii α_i sînt zero, fie $\alpha_k \neq 0$ cu k maxim. Atunci polinomul $\alpha_1f_1 + \ldots + \alpha_nf_n$ conține termenul $\alpha_kX^{m_k} \neq 0$. Contradicție.

37. $(q \circ q)(x) = q(q(x)) = q(x - p(x)) = x - p(x) + p(x) - p^2(x) = x - p(x) = q(x)$.

39. $f_\theta \circ f_{\theta'} = f_{\theta+\theta'}$, $g_\theta \circ g_{\theta'} = f_{\theta-\theta'}$, $f_\theta \circ g_{\theta'} = g_{\theta+\theta'}$, $g_\theta \circ f_{\theta'} = g_{\theta-\theta'}$ (v. și Ex. 6 și Ex. 17, Cap. I).

40. a) Dacă $\alpha \in \mathbf{R}$ și $u, v \in V$, $u = x + f(x)$, $v = y + f(y)$, atunci $u + v = (x + y) + f(x + y)$, $\alpha u = \alpha x + f(\alpha x)$; b) Dacă $x \in V$, atunci $y = \frac{1}{2}x + f\left(\frac{1}{2}x\right) \in V_1$, $z = \frac{1}{2}x - f\left(\frac{1}{2}x\right) \in V_2$ și $y + z = x$. Pentru unicitate, observați că $V_1 \cap V_2 = 0 = \{0\}$ c) Cînd $V = \mathbf{R}^2$ și $f = g_\pi$ avem $V_1 = \{(0, x_2) | x_2 \in \mathbf{R}\}$, $V_2 = \{(x_1, 0) \mid x_1 \in \mathbf{R}\}$.

42. 3) $\Rightarrow$ 2) Verificare; 2) $\Rightarrow$ 1) $\langle f_A(x),\ f_A(y)\rangle = \frac{1}{2}\ (\langle f_A(x+y),\ f_A(x+y)\rangle -$

$- \langle f_A(x),\ f_A(x)\rangle - \langle f_A(y),\ f_A(y)\rangle) = \frac{1}{2}\ (\langle x+y,\ x+y\rangle - \langle x,\ x\rangle - \langle y,\ y\rangle) = \langle x,\ y\rangle$;

1) $\Rightarrow$ 3) Fie $e_1 = (1, 0)$, $e_2 = (0, 1)$. Atunci $1 = \langle e_1,\ e_1\rangle = \langle f_A(e_1),\ f_A(e_1)\rangle = a^2 + c^2$, $0 = \langle e_1, e_2\rangle = \langle f_A(e_1), f_A(e_2)\rangle = ab + cd$, $1 = \langle e_2, e_2\rangle = \langle f_A(e_2), f_A(e_2)\rangle = b^2 + d^2$. Rezultă că ${}^TAA = E$. Se aplică apoi Ex. 19. Cap. I. Transformarea f_A reprezintă rotația de unghi θ în jurul originii (în sens invers acelor ceasornicului) cînd $\det(A) = 1$ și simetria față de dreapta ce trece prin origine și face unghiul $\theta/2$ cu Ox_1, cînd $\det(A) = -1$.

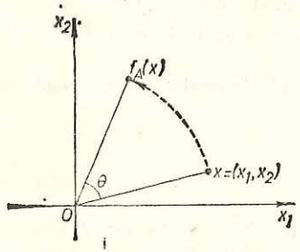


Fig. VI. 4

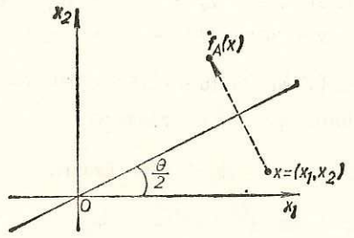


Fig. VI. 5

CUPRINS

Cap. I: **PRELIMINARII** 3

1. Numere 3
2. Mulțimi și funcții (recapitulare) 4
3. Matrice (recapitulare) 5
4. Numere relativ prime (recapitulare) 7
5. Numere pătratice 8

Exerciții 14

Cap. II: **LEGI DE COMPOZIȚIE**

1. Noțiunea de lege de compoziție. Exemple 17
2. Parte stabilă. Lege de compoziție indusă 19
3. Tabla unei legi de compoziție 20
4. Asociativitate 22
5. Comutativitate 23
6. Element neutru 26
7. Elemente simetrizabile 27
8. Proprietăți ale adunării și înmulțirii modulo n 30
9. Sume și produse iterate 34

Exerciții 37

Cap. III: **GRUPURI**

1. Metoda axiomatică în algebră 41
2. Monoizi 42
3. Definiția grupului. Exemple 45
4. Reguli de calcul într-un grup 48
5. Subgrup. Exemple 52
6. Morfisme de grupuri 55

Exerciții 60

Cap. IV: **INELE ȘI CORPURI**

1. Definiția inelului. Exemple 66
2. Reguli de calcul într-un inel 69
3. Inelul claselor de resturi modulo n 71
4. Corpuri 77
5. Morfisme de inele și corpuri 80

Exerciții 86

Cap. V: **POLINOAME**

1. Inele de polinoame 92
2. Teorema împărțirii cu rest 99
3. Divizori de grad 1 102

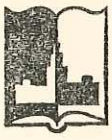
4. Relația de divizibilitate pentru polinoame cu coeficienți într-un corp 105
5. Algoritmul lui Euclid 107
6. Polinoame ireductibile 110
7. Descompunerea polinoamelor în produs de factori ireductibili 113
8. Rădăcini multiple 115
9. Relații între rădăcini și coeficienți 118
10. Rădăcini ale polinoamelor cu coeficienți rationali 121
Exerciții 124

Cap. VI: **SPAȚII VECTORIALE**

1. Legi de compoziție externe 129
2. Definiția spațiului vectorial 131
3. Dependență și independență liniară. Bază 134
4. Proprietăți ale sistemelor liniar independente (dependente). Coordonate 140
5. Lema substituției 145
6. Transformări liniare 151
Exerciții 153

Indicații și răspunsuri 160

Nr. colilor de tipar : 11
Bun de tipar: 24.12.1980



Com. nr. 655/27 400
Combinatul poligrafic
„CASA SCÎNTEII"
București — R.S.R.